

**RAMAKRISHNA MISSION
VIVEKANANDA CENTENARY
COLLEGE**



Name: Debarghya saha

Sem : 5th

Subject : CC-XII Project

Regn no : A01-1122-113-001-2019

Roll : 2022151091

Burnside's Lemma

Preface: Burnside Lemma is also known as Burnside's counting theorem, Cauchy – Frobenius lemma also as “The Lemma that is not Burnside's” is one of the important results, more specifically a way that relates both algebra and geometry. This lemma was attributed to Frobenius in the book on finite groups by Burnside himself. Though, there are several confusions, that this lemma was known to Cauchy in 1845.



William Burnside



Augustin Louis Cauchy

Introduction: Burnside theorem is not only used in algebra but also in organic chemistry also in our daily life. There are some uses of finding isomers of organic molecule in chemistry. We also use this lemma in necklace problem, it gives us the exact number of distinct colorings, but it does not include information on the type of configuration. Polya's enumeration theorem weights the colors in one or more ways, so there could be any number of colors given the set of colors has generation function with finite coefficients.

Polya's Enumeration Formula : a Let X be a set of elements and G be a group of permutations of X that lead to equivalent colourings of X. We will use the colours W1, W2...Wm and this can be expressed by the following generating function, where k is the largest cycle length.

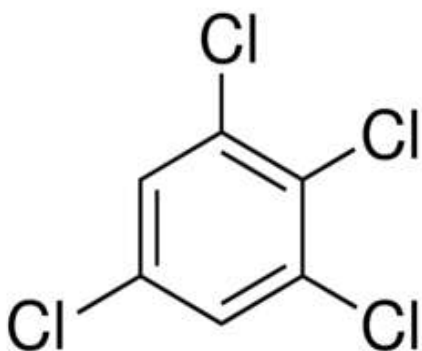
$$P_G (\sum_{j=1}^m w(j), \sum_{j=1}^m w(j)^2, \dots, \sum_{j=1}^m w(j)^k)$$

My idea

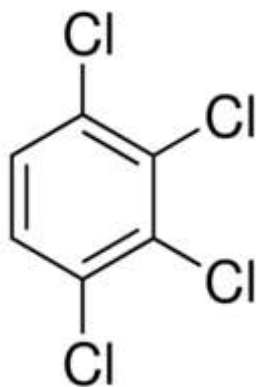
Applying Burnside Lemma we can solve many difficult problems in our daily life such as -Necklace problem, Rubik's cube problem, number of different coloured hexagon or polygon etc. But here we shall use the lemma in Chemical Isomer Enumeration and Music Theory Enumeration.

Chemical Isomer Enumeration

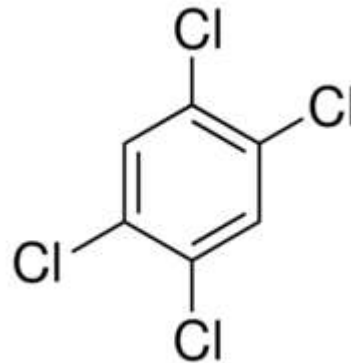
In this enumeration we can use Polya Enumeration Theorem which is an extent of Burnside lemma to enumerate these types of isomers. Let's took an example -the molecule **Tetra chlorobenzene $C_6H_2Cl_4$** has the following isomers.



1,2,3,5-tetrachlorobenzene



1,2,3,4-tetrachlorobenzene



1,2,4,5-tetrachlorobenzene

We can use Polya Enumeration Theorem to determine the number of ways of attaching two chlorine atoms and four hydrogen atoms onto the carbon ring. To do this, we assign numbers 1-6 for the six carbons of the hexagon, and Y be the set with a chlorine and hydrogen atom with weights Cl and H respectively.

Then, we get the configuration generating function:

$$\begin{aligned} F(H; Cl) &= ZC_6 (H + Cl; H^2 + Cl^2; \dots; H^6 + Cl^6) \\ &= 1/6((H + Cl)^6 + (H^2 + Cl^2)^3 + 2(H^3 + Cl^3)^2 + 2(H^6 + Cl^6)) \\ &= H^6 + H^5Cl + 3H^4Cl^2 + 4H^3Cl^3 + 3H^2Cl^4 + HCl^5 + Cl^6 \end{aligned}$$

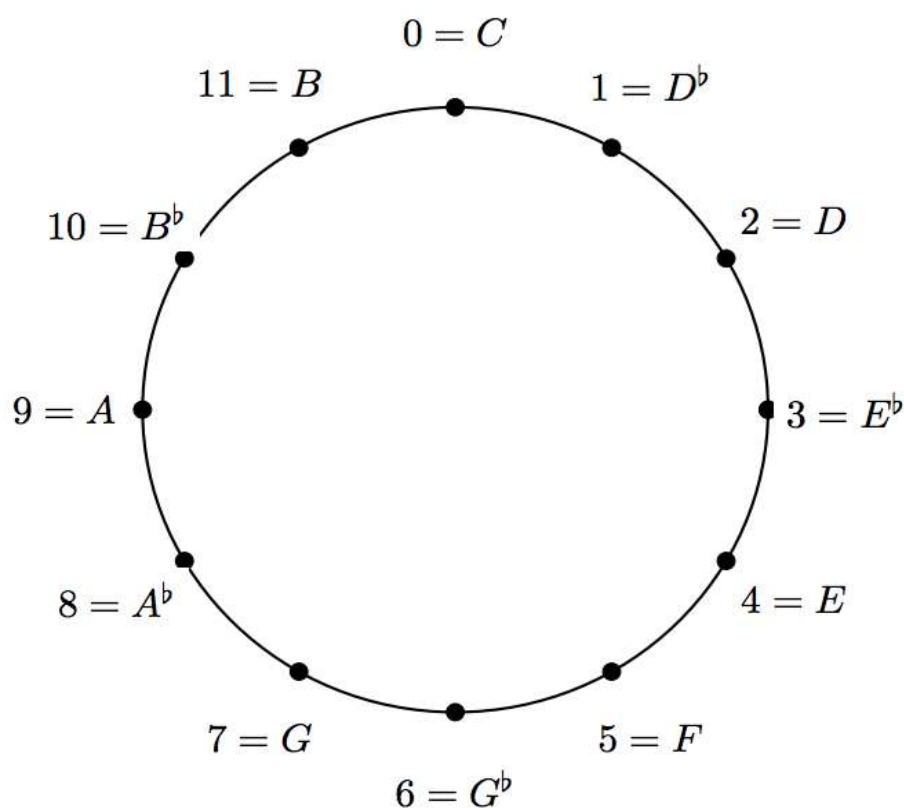
The coefficients in the generating function represent how many isomers exist for that chemical formula, so in this case the coefficient of H²Cl⁴ means that there are three isomers of tetra chlorobenzene which are shown in the diagram above.

Music Theory Enumeration

We can also apply this theorem to music theory in the enumeration of distinct chords.

In Western music, tones are equivalent if they differ by an octave. There are a total of 12 tones, which are **C; D^b; D; E^b; E; F; G^b; G; A^b; A; B^b; B**. The tones are typically arranged in a circle to show that they cycle through an octave.

The tones are shown on the following page, represented as numbers from 0 to 12.



We will look more closely at triads, which are a subset of tones made with three distinct tones. We will consider two triples to be equivalent if one can be translated to another. For example, the two chords $[D, F, A] = [2, 5, 9]$ and $[E, G, B] = [4, 7, 11]$ would be considered equivalent because the $[E, G, B]$ chord is a shift of 2 tones above each note in the first chord. Thus, if the spaces between the triads are equal then the chord has simply been translated. In addition, triples are equivalent if the tones are permuted with the same set of notes. For example, $[D, F, A] = [2, 5, 9]$ is the same as the chord $[A, F, D] = [9, 5, 2]$ because they consist of the same notes, just in a different ordering.

This is called an inversion.

To solve this, we can use Burnside's Lemma. Let X be the set of all distinct triples of elements from Z . If we consider all the ways to select three tones from a set of 12 tones regardless of ordering, we get $|X| = {}^{12}C_3$.

Because it does not account for ordering, this already eliminates the problem of different chord permutations and does not double count these. Thus, the only other transformation we need to account for is translation of the chords. We can represent this as

$$\{(a; b; c); k\} = \{a + k; b + k; c + k\}$$

We need to determine the number of distinct orbits to determine the number of different triads we can make.

To do this, we identify the elements of our group:

1. $k = 0$ (Identity Transformation)

All of these are fixed points because nothing is changed after the identity transformation, so $|X| = {}^{12}C_3$

2. $k = 4$

This will lead to a fixed point if and only if the following equation holds true

$$4\{a; b; c\} = \{a + 4; b + 4; c + 4\} = \{a; b; c\}$$

This results in four triples, so $|X^4| = 4$

3. $k = 8$

Using the same reasoning as above, we also have $|X^8| =$

4. These are the only possible fixed points that exist because in any d -tone system where we are selecting n -tuples of tones, the only value k that we can

have fixed points is when kn is a multiple of d . In this situation, we have a 12-tone system and we are selecting 3 tuples of tones. So, this means that the only possible fixed points is when $3k$ is a multiple of 12, so when $k = 0,4,8$.

Using Burnside's Lemma, we calculate that the number of distinct orbits, which represent the number of distinct triads, is equal to

$$\begin{aligned} 1/|G| \sum_{g \in G} |x^g| &= 1/12(x^0 + x^4 + x^8) \\ &= ({}^{12}C_3 + 4 + 4)/12 \\ &= 228/12 = 19 \end{aligned}$$

This represents the number of distinct triads for triples, but similar methods can be used to enumerate the different n -tuples tones as well.

Conclusion :-

We have discussed applications of Burnside Lemma and Polyá Enumeration theorem in this project. . We have noticed that we can only count the number of distinct colourings by Burnside Lemma and to know about their configuration we have to use Polyá Enumeration theorem. Then we have described the Polyá Enumeration theorem shortly and from its many fields of applications we have chosen Chemical Isomer Enumeration and Music theory Enumeration for discussion. Since in chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecules in space which are called isomers, we can use Polyá Enumeration Theorem to enumerate these types of isomers. In music theory, Polyá Enumeration theorem is used to identify patterns within chord sequences, in addition to counting the number of patterns in intervals and rhythms.

Acknowledgement

I would love to reveal remarkable and extra special thanks to Dr. Pravanjan Kumar Rana, head of the department Mathematics of Ramakrishna Mission Vivekananda Centenary College, Rahara; who gave me a very good opportunity to work on this project and his helpful behaviour helps me to complete this project.

I would also love to thank my group partners (Parthib Paul and Ayan Sarkar) who had helped me a lot in this project.

Project work
Submitted for partial fulfillment of the B.Sc. Degree
in Mathematics



Under the supervision of Dr. Pravanjan Kumar Rana

By: -

Name: - Suman Parui

Reg. No.: - A01-1112-113-002-2019

Examination Roll no.: - 2022151092

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata- 700118

ACKNOWLEDGEMENT

I would love reveal remarkable and extra special thanks to Dr. Pravanjan Kumar Rana, head of the department mathematics of RKMVCC Rahara, who gave me a very good opportunity to work on this project and with that his helpful behaviour helps me to complete this project.

I would also love to thank my group partners (Raj Das and Soubhik Mandal) who helped me a lot on this project.

“Visual Interpretation of Sylow’s Theorem”

Key highlights: -

- *Introduction*
- *p -groups*
- *Sylow’s Theorem with visual interpretation*
- *Conclusion*
- *References*

INTRODUCTION

The **Sylow's theorems** are important tools in finite group theory. The **Lagrange's theorem** tells us that the order of a subgroup of a finite group is a divisor of the order of that group. The converse, however, is false. There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. The most basic and widely used, is a classic theorem due to the **Norwegian mathematician Sylow**.

There are three proofs of this result of Sylow. The **first** is a very elegant and elementary argument due to **Wielandt**. It appeared in the journal *Archiv der Mathematik*, vol. 10 (1959), pages 401-402. The basic elements in Wielandt's proof are number-theoretic and combinatorial. It has the advantage, aside from its elegance and simplicity, of producing the subgroup we are seeking. The **second** proof is based on an exploitation of induction in an interplay with the **class equation**. It is one of the standard classical proofs, and is a nice illustration of the combining many of the ideals developed so far to derive this very important cornerstone due to Sylow. The **third** proof is of a completely different philosophy. The basic idea there is to show that if a larger group than the one we are considering satisfies the conclusion of the Sylow's theorem, then our group also must. This forces us to prove Sylow's theorem for a special family of groups—the symmetric groups. By invoking Cayley's Theorem, we are then able to deduce Sylow's theorem for all finite groups. Apart from this strange approach—to prove something for a given group, first prove it for a much larger one—this third proof has its own advantages. Exploiting the ideas used, we easily derive the so-called **second and third parts** of Sylow's theorem. Here we discuss about the classical proof of Sylow's theorem with visual interpretation.

p-groups

Definition: (p-groups, p-subgroups):

A p-group is a group whose order is a power of a prime p, A p-group \equiv that is a subgroup of group G is called p-subgroup of G.

For example, D_4 is a 2-group, because its order is 8, a power of the prime 2. It contains a subgroup isomorphic to C_4 , which is therefore a 2-subgroup of D_4 because its order 2^2 . Similarly, C_1 and C_{13} are both 13-groups, because their orders are powers of the prime 13 (specifically, 13^0 and 13^1).

Theorem 1: If a p-group G acts on a set S, then the order of S and the number of stable elements in S are congruent mod p.

Theorem 2: If H is a p-subgroup of G, then $[N_G(H):H] \equiv_p [G:H]$

$[G:H]$ is the number of left cosets of H in G. Thus, the theorem says that whether we count only those cosets in the normalizer $N_G(H)$ or all the cosets in G, the result is the same mod p.

This theorem is here because the First Sylow theorem depends on it.

Proof: Let S be the left cosets of H in G and consider the group H acting on S by the interpretation homomorphism $\Phi: G \rightarrow \text{perm}(S)$ defined by

$$\Phi(h) = \text{the permutation that sends a coset } gH \text{ to the coset } hgH.$$

In such a situation We say that G acts on S by “by left multiplication” I can prove that its stable elements are just those left cosets in the normalizer, as shown in the figure 1.

Now the left cosets of H in $N_G(H)$ are those left cosets that are also right cosets. Figure 2 illustrates and explains why they are also those cosets stabilized by the above group action. The explanations in that figure are an important part of this proof. Since the stable elements are those cosets in $N_G(H)$, the number of them is $[N_G(H):H]$.

The final step of the strategy is to apply theorem 1, which tells us that the number of stable elements must be congruent mod p to $|S|$, which in this case

Is the number of left cosets of H , $[G:H]$, writing this as an equation yields the statement of the theorem;

$$[N_G(H): H] \equiv_p [G:H].$$

Figure 1: When H acts on its cosets by left multiplication, the stable element s are exactly those elements in its normalizer $N_G(H)$.

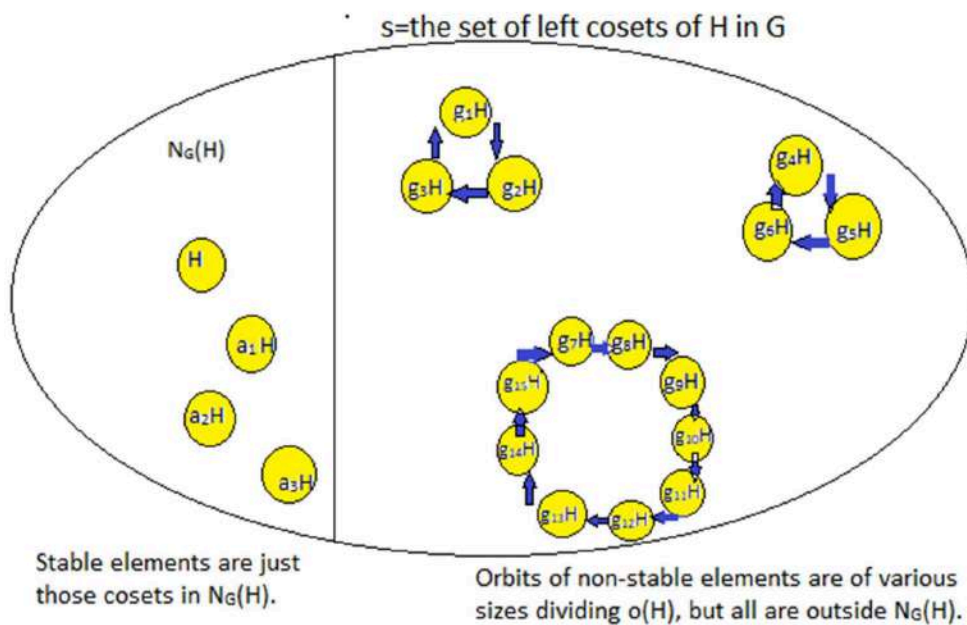


Figure:1

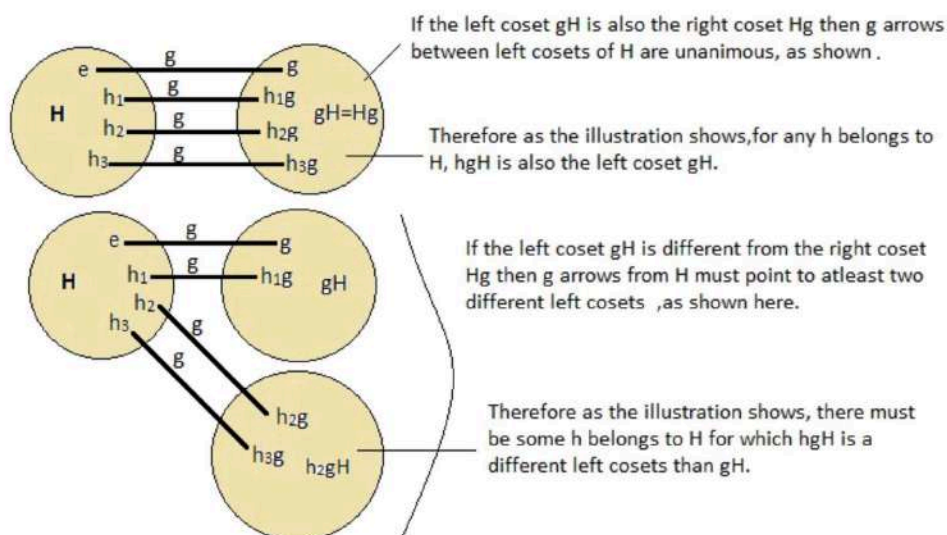


Figure 2

Sylow's Theorem with Visual Interpretation

If G is a Finite group of order n and if H is a subgroup of G , then we know by Lagrange's theorem that the order of H divides n . Sylow's Theorem gives the answer to the question, "If m is a positive integer, which divides n , does G contain a subgroup of order of m ?". The Sylow Theorems give us the following three kinds of information about the p -subgroups of any group.

1. **Existence:** In every group, p -subgroups of all possible sizes are guaranteed to exist.
 2. **Relationship:** A group's p -subgroups have ties to one another through conjugacy.
 3. **Number:** There are restrictions on how many p -subgroups a group can have.
- **Sylow's First Theorem:** Let G be a finite group of order $p^r m$, where p is a prime, r and m are positive integers, and p and m are relatively prime. Then G has a subgroup of order p^k for all k , $0 \leq k \leq r$.

The First Sylow Theorem generalizes **Cauchy's Theorem** [If p is a prime number that divides $O(G)$, then G has an element g of order p , and therefore a subgroup $\langle g \rangle$ of order p .] in several ways, summarized in Table 1, its proof deals with both statements in the theorem at once by using Cauchy's Theorem to expand smaller p -subgroup to create larger ones. The First Sylow tells us a bit about the relationship among p -subgroups, but we will learn more about that relationship from Second Sylow Theorem.

Proof.

It is easy to find a p -subgroup of order 1 (which is p^0) because it is obviously

Cauchy's Theorem	First Sylow Theorem
If p divides $O(G)$, then there is a subgroup of order p .	If p^i divides $O(G)$, then there is a subgroup of order p^i .

<i>It is cyclic and has no subgroups.</i>	<i>Each has subgroups of orders 1, p, p^2, up to p^i.</i>
<i>There is also an element of order p.</i>	<i>There is not necessarily an element of order p^i.</i>

$\{e\}$. We also know that there is a p -subgroup of order p (which is p^1) from Cauchy's Theorem (as long as $O(G) > 1$). The main job of this proof is showing the existence of the larger subgroups, by explaining how to make any $H < G$ of any order $p^i < p^n$ and expand it to create a new subgroup $H^* < G$ that contains H and is p times as large, as shown in the given figure. We can then repeatedly expand the smallest p -subgroups, creating larger ones up to size p^n .

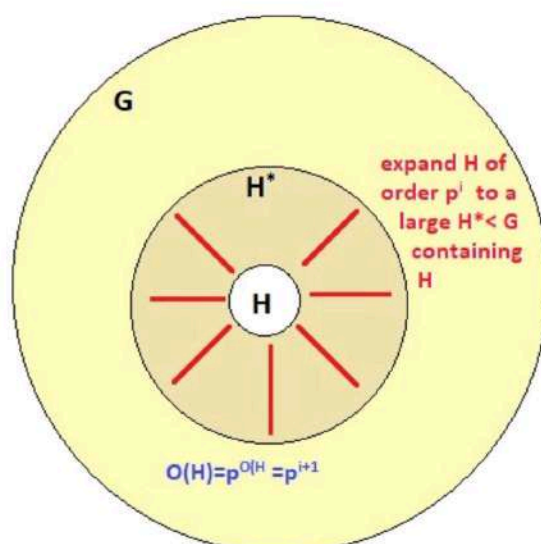


Figure: First Sylow Theorem gives a procedure for taking a subgroup of order p^i and finding a larger subgroup whose order is p^{i+1} (as long as p^{i+1} divides $O(G)$).

We can find the H^* we seek inside the normalizer $N_G(H)$ by relying on the fact that $H \triangleleft N_G(H)$. Next figure illustrates the groups, subgroups, and homomorphism that come into play in the rest of this proof; refer to it help **visualize** the following argument. Create the quotient group $N_G(H)/H$ and call the quotient map q . The size of the quotient group is the number of cosets of H in its normalizer, $[N_G(H):H]$, which Theorem 2 says must be congruent to $[G:H] \pmod{p}$. So, what do we know about $[G:H]$? We're given that the order of G is some multiple of p^n , say $p^n m$. So, the number of cosets of H is

$$[G:H] = O(G)/O(H) = p^n m / p^i = p^{n-i} m.$$

Because $p^i < p^n$, we know that $p^{n-i} > 1$ and so p divides $p^{n-i} m$. Therefore $[G:H]$ and $[N_G(H):H]$ are both multiples of p . The order of $N_G(H)/H$ is obviously not 0, so it must be a positive multiple of p . This lets us use Cauchy's theorem to find an element of order p in the quotient group; call that element aH . The cyclic subgroup $\langle aH \rangle$ will be very useful to us. The collection of elements that q maps to $\langle aH \rangle$ obviously contains H , but as the Figure suggests it is also a subgroup of $N_G(H)$.

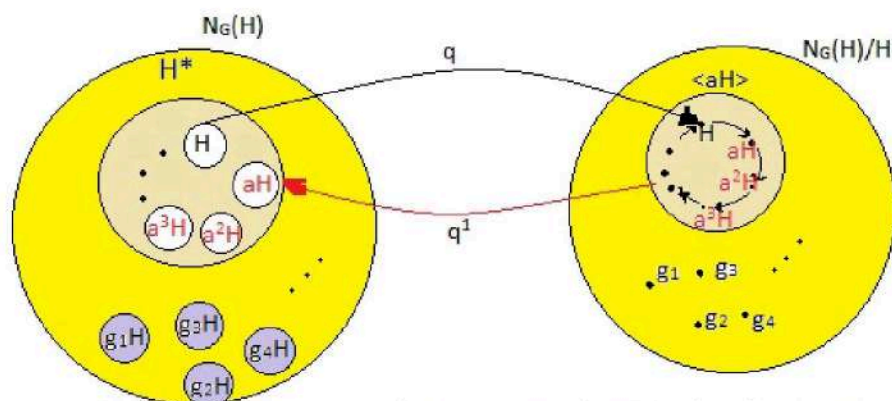


Figure: The quotient map and its inverse used in First Sylow theorem to create a subgroup H^* whose order is p times of H

It is the subgroup H^* that we seek; it contains H and has size p^{i+1} for the following reason. There are p elements in $\langle aH \rangle$, and therefore p cosets of H in H^* . Since H contains p^i elements, each of its cosets does as well, and H^* contains p of them, for a total of p^{i+1} elements. The preceding paragraphs give a way to expand any H of order $p^i < p^n$ into a larger H^* of order p^{i+1} . Beginning with $H = \{e\}$, we can repeatedly expand it to create H^* , H^{**} , and so on of orders p , p^2 , up to p^n .

The expansion technique in this proof is an example of conjugacy. It applies q to H , applies Cauchy's theorem in the quotient group to turn one element into p elements, and applies q^{-1} to bring those p elements back into G , as p cosets

forming a subgroup H^* . Even though q^{-1} isn't really a function, this is a useful way to summarize the argument.

Now we discuss Second and third part of Sylow's Theorem shortly:

- **The Second Sylow Theorem: Relationship among p-subgroups:**

The First Sylow Theorem guarantees the existence of subgroups of certain sizes, and what it told us of the relationship among such groups was that all smaller p -subgroups are inside larger ones. The Second Sylow Theorem shows us how the largest such p -subgroups relate through conjugacy.

Definition: (Sylow p -subgroup): We call H a Sylow p -subgroup of G if it is a p -subgroup whose order is the highest power of p that divides $O(G)$. In other words, H is a p -subgroup of G that's either the largest one, or tied for it.

Theorem:(Sylow's Second Theorem): Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then any two Sylow's p -subgroups of G are **conjugate**, and therefore **isomorphic**.

Here we mention some of its important consequences that may not at first be obvious. Conjugating by any group element creates an isomorphism from the group to itself called an inner automorphism. Thus, when two subgroups are conjugates (say $H = gKg^{-1}$), there is an inner automorphism mapping one to the other ($\Phi(x) = gxg^{-1}$). Therefore, conjugate subgroups are isomorphic.

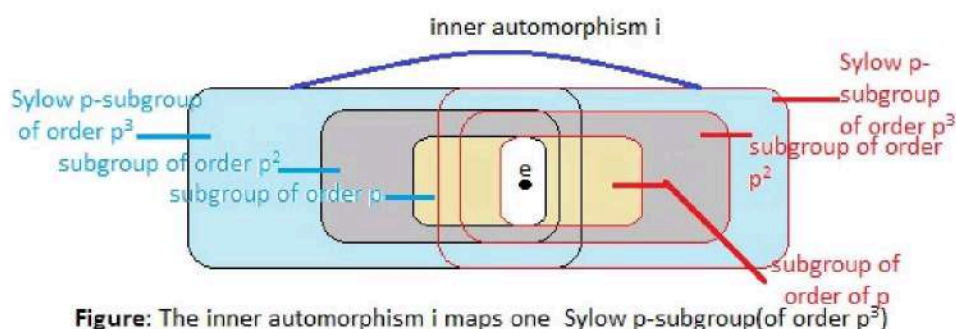


Figure: The inner automorphism i maps one Sylow p -subgroup(of order p^3) to another, which therefore has identical internal structure.

The Second Sylow Theorem tells us that all of a group's largest p -subgroups are one another's conjugates, and so they are all isomorphic to one another. Now recall the nesting relationship among p -subgroups given by the First Sylow Theorem, so that every p -subgroup is inside a Sylow p -subgroup. Conjugating any Sylow p -subgroup by any group element results in a (possibly different) Sylow p -subgroup, with identical internal structure, as shown in the Figure.

Therefore, any smaller p -subgroup must have a copy of itself (one of its conjugates) in every Sylow p -subgroup.

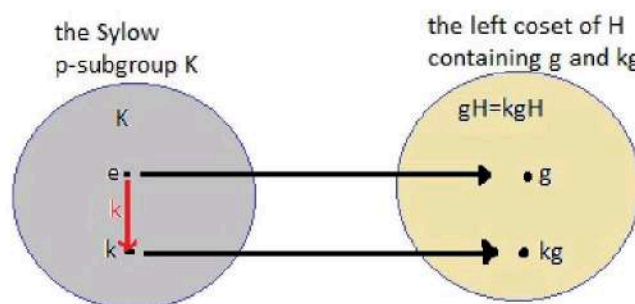


Figure: A stable element gH of the group action in the proof of the Second Sylow Theorem is one for which, for any k belong to K , $kgH=gH$.

it appears to intersect the original Sylow 2-subgroup only at the identity, that is just one possibility. For instance, if $\langle a \rangle$ were a normal subgroup, then it would be conjugate only to itself, so every Sylow 2-subgroup would contain all of $\langle a \rangle$.

- **Sylow's Third Theorem: Number of p -subgroups:**

Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then the number n_p of Sylow p Subgroups of G is $1+kp$ for some nonnegative integer k and $n_p \mid p^r m$

This theorem helps us narrow down, just based on a group's order, the possible number of Sylow p -subgroups that the group can have. It does not always narrow down the possibilities to only one number, but it is often a big improvement over no information at all.

Conclusion

The Sylow's Theorems are a powerful statement about the structure of groups in general, but are also powerful in applications of finite group theory.

Sometimes we need visualize concepts to understand the topic deeply. First, we introduce p -groups, some necessary Theorems. Then discuss Sylow's theorems with visualization. That's all from our project work.

References

- *Visual Group Theory* by Nathan C. Carter, Bentley University.
- *Topics In Algebra* by I. N. Herstein, University of Chicago.
- *Fundamentals of Abstract Algebra*, D.S. Malik (Creighton University), John M. Mordeson (Creighton University), M.K. Sen (Calcutta University).



RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE

A PROJECT ON THE APPLICATION OF BURNSIDE LEMMA

NAME- **PARTHIB PAUL**

SEMESTER- **5th(B.SC)**

COLLEGE ROLL NO.-**304**

EXAM ROLL NO.-**2022151093**

REG. NO.-**A01-1112-113-003-2019**

PAPER CODE-**MTMA CC-XII**

SUPERVISED BY-**DR. PRAVANJAN KUMAR RANA**

Burnside's Lemma

Preface: Burnside Lemma is also known as Burnside's counting theorem, Cauchy – Frobenius lemma also as “The Lemma that is not Burnside's” is one of the important results, more specifically a way that relates both algebra and geometry. This lemma was attributed to Frobenius in the book on finite groups by Burnside himself. Though, there are several confusions, that this lemma was known to Cauchy in 1845.



William Burnside



Augustin Louis Cauchy

Introduction: Burnside theorem is not only used in algebra but also in organic chemistry also in our daily life. There are some uses of finding isomers of organic molecule in chemistry. We also use this lemma in necklace problem, it gives us the exact number of distinct colorings, but it does not include information on the type of configuration. Polya's enumeration theorem weights the colors in one or more ways, so there could be any number of colors given the set of colors has generation function with finite coefficients.

Polya's Enumeration Formula : a Let X be a set of elements and G be a group of permutations of X that lead to equivalent colourings of X. We will use the colours W1, W2...Wm and this can be expressed by the following generating function, where k is the largest cycle length.

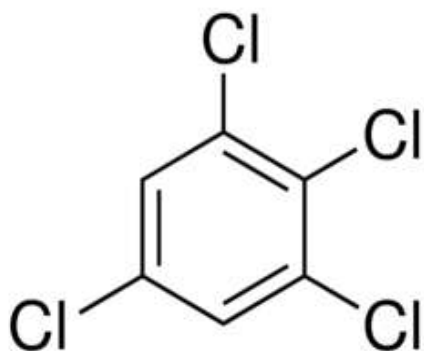
$$P_G (\sum_{j=1}^m w(j), \sum_{j=1}^m w(j)^2, \dots, \sum_{j=1}^m w(j)^k)$$

My idea

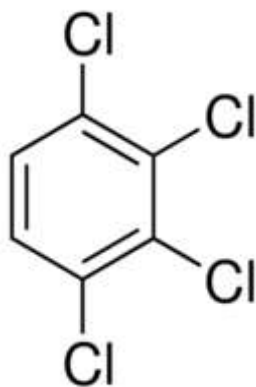
Applying Burnside Lemma we can solve many difficult problems in our daily life such as -Necklace problem, Rubik's cube problem, number of different coloured hexagon or polygon etc. But here we shall use the lemma in Chemical Isomer Enumeration and Music Theory Enumeration.

Chemical Isomer Enumeration

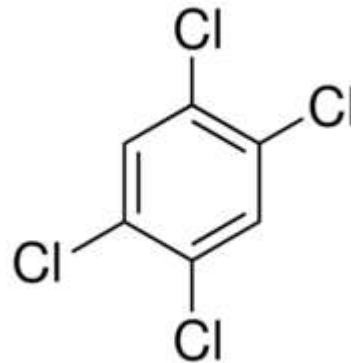
In this enumeration we can use Polya Enumeration Theorem which is an extent of Burnside lemma to enumerate these types of isomers. Let's took an example -the molecule **Tetra chlorobenzene $C_6H_2Cl_4$** has the following isomers.



1,2,3,5-tetrachlorobenzene



1,2,3,4-tetrachlorobenzene



1,2,4,5-tetrachlorobenzene

We can use Polya Enumeration Theorem to determine the number of ways of attaching two chlorine atoms and four hydrogen atoms onto the carbon ring. To do this, we assign numbers 1-6 for the six carbons of the hexagon, and Y be the set with a chlorine and hydrogen atom with weights Cl and H respectively.

Then, we get the configuration generating function:

$$\begin{aligned} F(H; Cl) &= ZC_6(H + Cl; H^2 + Cl^2; \dots; H^6 + Cl^6) \\ &= 1/6((H + Cl)^6 + (H^2 + Cl^2)^3 + 2(H^3 + Cl^3)^2 + 2(H^6 + Cl^6)) \\ &= H^6 + H^5Cl + 3H^4Cl^2 + 4H^3Cl^3 + 3H^2Cl^4 + HCl^5 + Cl^6 \end{aligned}$$

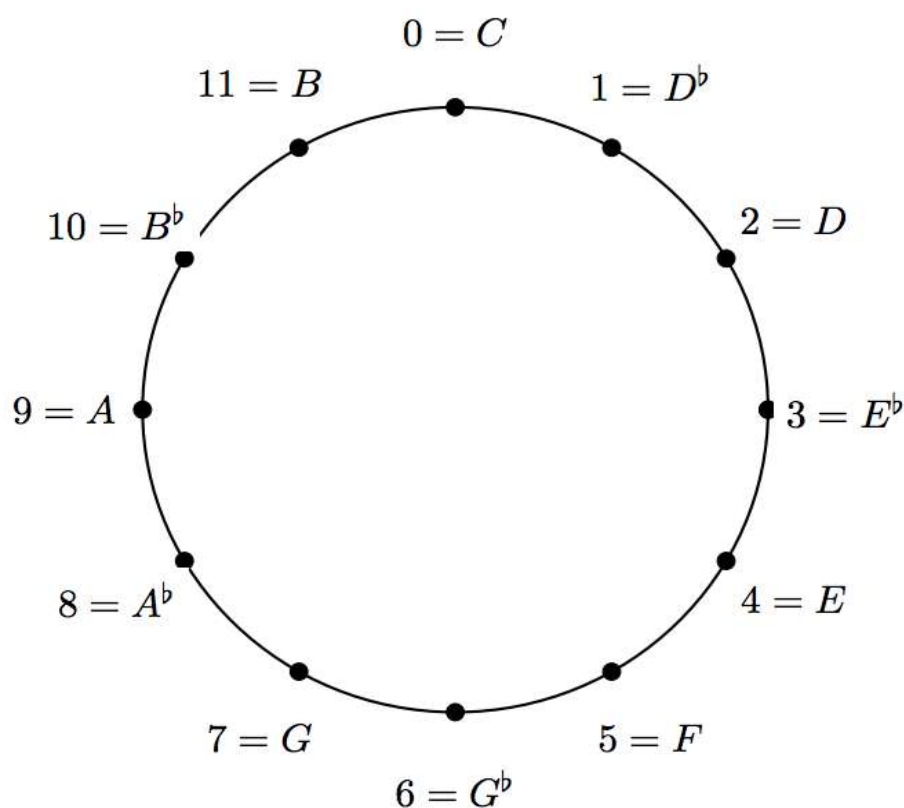
The coefficients in the generating function represent how many isomers exist for that chemical formula, so in this case the coefficient of H^2Cl^4 means that there are three isomers of tetra chlorobenzene which are shown in the diagram above.

Music Theory Enumeration

We can also apply this theorem to music theory in the enumeration of distinct chords.

In Western music, tones are equivalent if they differ by an octave. There are a total of 12 tones, which are **C; D^b; D; E^b; E; F; G^b; G; A^b; A; B^b; B**. The tones are typically arranged in a circle to show that they cycle through an octave.

The tones are shown on the following page, represented as numbers from 0 to 12.



We will look more closely at triads, which are a subset of tones made with three distinct tones. We will consider two triples to be equivalent if one can be translated to another. For example, the two chords $[D, F, A] = [2, 5, 9]$ and $[E, G, B] = [4, 7, 11]$ would be considered equivalent because the $[E, G, B]$ chord is a shift of 2 tones above each note in the first chord. Thus, if the spaces between the triads are equal then the chord has simply been translated. In addition, triples are equivalent if the tones are permuted with the same set of notes. For example, $[D, F, A] = [2, 5, 9]$ is the same as the chord $[A, F, D] = [9, 5, 2]$ because they consist of the same notes, just in a different ordering.

This is called an inversion.

To solve this, we can use Burnside's Lemma. Let X be the set of all distinct triples of elements from Z . If we consider all the ways to select three tones from a set of 12 tones regardless of ordering, we get $|X| = {}^{12}C_3$.

Because it does not account for ordering, this already eliminates the problem of different chord permutations and does not double count these. Thus, the only other transformation we need to account for is translation of the chords. We can represent this as

$$\{(a; b; c); k\} = \{a + k; b + k; c + k\}$$

We need to determine the number of distinct orbits to determine the number of different triads we can make.

To do this, we identify the elements of our group:

1. $k = 0$ (Identity Transformation)

All of these are fixed points because nothing is changed after the identity transformation, so $|X| = {}^{12}C_3$

2. $k = 4$

This will lead to a fixed point if and only if the following equation holds true

$$4\{a; b; c\} = \{a + 4; b + 4; c + 4\} = \{a; b; c\}$$

This results in four triples, so $|X^4| = 4$

3. $k = 8$

Using the same reasoning as above, we also have $|X^8| =$

4. These are the only possible fixed points that exist because in any d -tone system where we are selecting n -tuples of tones, the only value k that we can

have fixed points is when kn is a multiple of d . In this situation, we have a 12-tone system and we are selecting 3 tuples of tones. So, this means that the only possible fixed points is when $3k$ is a multiple of 12, so when $k = 0,4,8$.

Using Burnside's Lemma, we calculate that the number of distinct orbits, which represent the number of distinct triads, is equal to

$$\begin{aligned} 1/|G| \sum_{g \in G} |x^g| &= 1/12(x^0 + x^4 + x^8) \\ &= ({}^{12}C_3 + 4 + 4)/12 \\ &= 228/12 = 19 \end{aligned}$$

This represents the number of distinct triads for triples, but similar methods can be used to enumerate the different n -tuples tones as well.

Conclusion :-

We have discussed applications of Burnside Lemma and Polya Enumeration theorem in this project. We have noticed that we can only count the number of distinct colourings by Burnside Lemma and to know about their configuration we have to use Polya Enumeration theorem. Then we have described the Polya Enumeration theorem shortly and from its many fields of applications we have chosen Chemical Isomer Enumeration and Music theory Enumeration for discussion. Since in chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecules in space which are called isomers, we can use Polya Enumeration Theorem to enumerate these types of isomers. In music theory, Polya Enumeration theorem is used to identify patterns within chord sequences, in addition to counting the number of patterns in intervals and rhythms.

References

[1] Polya Enumeration Theorem :

https://en.wikipedia.org/wiki/P%C3%B3lya_enumeration_theorem

[2] Matias von Bell. Polya's Enumeration Theorem and its Applications. Dec, 2015.

• <https://helda.helsinki.fi/bitstream/handle/10138/159032/GraduTiivistelma.pdf?sequence=3>

[3] Harald Friertinger and Graz Voitsberg.

Enumeration in Music Theory

• <http://emis.math.tifr.res.in/journals/SLC/opapers/s26friert.pdf>

Acknowledgement

I would love to reveal remarkable and extra special thanks to Dr. Pravanjan Kumar Rana, head of the department Mathematics of Ramakrishna Mission Vivekananda Centenary College, Rahara; who gave me a very good opportunity to work on this project and his helpful behaviour helps me to complete this project.

I would also love to thank my group partners (Ayan Sarkar and Debarghya Saha) who had helped me a lot in this project.



Department of Mathematics

**Ramakrishna Mission Vivekananda Centenary
College**

Rahara, Kolkata- 700118

Project Work

**Submitted for partial fulfillment of the B.Sc. Degree
In Mathematics**

Under the supervision of Dr. Pravanjan Kumar Rana

- Name: - Ayan Sarkar
- Reg. No.: - A01-1112-113-004-2019
- Examination Roll No: - 2022151094

Acknowledgement

I would love to reveal remarkable and extra special thanks to Dr. Pravanjan Kumar Rana, head of the department Mathematics of Ramakrishna Mission Vivekananda Centenary College, Rahara; who gave me a very good opportunity to work on this project and his helpful behaviour helps me to complete this project.

I would also love to thank my group partners (Parthib Paul and Debarghya Saha) who had helped me a lot in this project.

Burnside's Lemma

❖ **Preface:** Burnside Lemma is also known as Burnside's counting theorem, Cauchy – Frobenius lemma also as “The Lemma that is not Burnside's” is one of the important results, more specifically a way that relates both algebra and geometry. This lemma was attributed to Frobenius in the book on finite groups by Burnside himself. Though, there are several confusions, that this lemma was known to Cauchy in 1845.



William Burnside



Augustin Louis Cauchy

➤ **Introduction:** Burnside theorem is not only used in algebra but also in organic chemistry also in our daily life. There are some uses of finding isomers of organic molecule in chemistry. We also use this lemma in necklace problem, it gives us the exact number of distinct colorings, but it does not include information on the type of configuration. Polya's enumeration theorem weights the colors in one or more ways, so there could be any number of colors given the set of colors has generation function with finite coefficients.

Polya's Enumeration Formula : Let X be a set of elements and G be a group of permutations of X that lead to equivalent colourings of X. We will use the colours W_1, W_2, \dots, W_m and this can be expressed by the following generating function, where k is the largest cycle length.

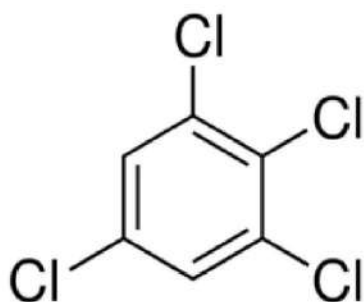
$$P_G \left(\sum_{j=1}^m w(j), \sum_{j=1}^m w(j)^2, \dots, \sum_{j=1}^m w(j)^k \right)$$

My idea

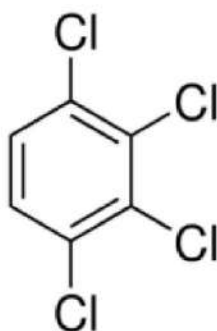
Applying Burnside Lemma we can solve many difficult problems in our daily life such as -Necklace problem, Rubik's cube problem, number of different coloured hexagon or polygon etc. But here we shall use the lemma in Chemical Isomer Enumeration and Music Theory Enumeration.

Chemical Isomer Enumeration

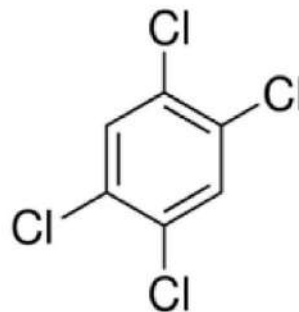
In this enumeration we can use Polya Enumeration Theorem which is an extent of Burnside lemma to enumerate these types of isomers. Let's took an example -the molecule **Tetra chlorobenzene $C_6H_2Cl_4$** has the following isomers.



1,2,3,5-tetrachlorobenzene



1,2,3,4-tetrachlorobenzene



1,2,4,5-tetrachlorobenzene

We can use **Polya Enumeration Theorem** to determine the number of ways of attaching two chlorine atoms and four hydrogen atoms onto the carbon ring. To do this, we assign numbers 1-6 for the six carbons of the hexagon, and Y be the set with a chlorine and hydrogen atom with weights Cl and H respectively.

Then, we get the configuration generating function:

$$\begin{aligned} F(H; Cl) &= ZC_6 (H + Cl; H^2 + Cl^2; \dots; H^6 + Cl^6) \\ &= 1/6((H + Cl)^6 + (H^2 + Cl^2)^3 + 2(H^3 + Cl^3)^2 + 2(H^6 + Cl^6)) \\ &= H^6 + H^5Cl + 3H^4Cl^2 + 4H^3Cl^3 + 3H^2Cl^4 + HCl^5 + Cl^6 \end{aligned}$$

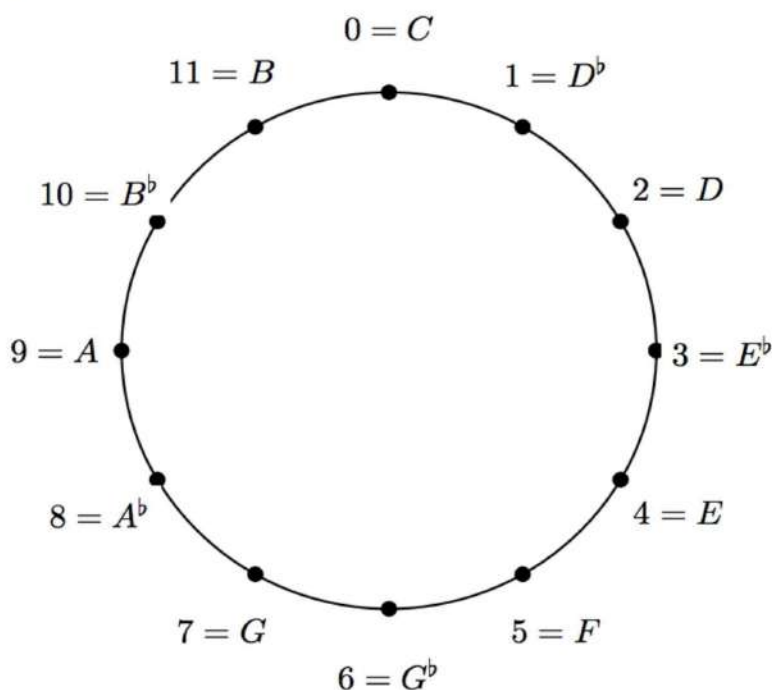
The coefficients in the generating function represent how many isomers exist for that chemical formula, so in this case the coefficient of H^2Cl^4 means that there are three isomers of tetra chlorobenzene which are shown in the diagram above.

Music Theory Enumeration

We can also apply this theorem to music theory in the enumeration of distinct chords.

In Western music, tones are equivalent if they differ by an octave. There are a total of 12 tones, which are **C; D^b; D; E^b; E; F; G^b; G; A^b; A; B^b; B**. The tones are typically arranged in a circle to show that they cycle through an octave.

The tones are shown on the following page, represented as numbers from 0 to 12.



We will look more closely at triads, which are a subset of tones made with three distinct tones. We will consider two triples to be equivalent if one can be translated to another. For example, the two chords $[D, F, A] = [2, 5, 9]$ and $[E, G, B] = [4, 7, 11]$ would be considered equivalent because the $[E, G, B]$ chord is a shift of 2 tonnes above each note in the first chord. Thus, if the spaces between the triads are equal then the chord has simply been translated. In addition, triples are equivalent if the tones are permuted with the same set of notes. For example, $[D, F, A] = [2, 5, 9]$ is the same as the chord $[A, F, D] = [9, 5, 2]$ because they consist of the same notes, just in a different ordering.

This is called an inversion.

To solve this, we can use Burnside's Lemma. Let X be the set of all distinct triples of elements from Z . If we consider all the ways to select three tones from a set of 12 tones regardless of ordering, we get $|x| = ({}^{12}C_3)$.

Because it does not account for ordering, this already eliminates the problem of different chord permutations and does not double count these. Thus, the only other transformation we need to account for is translation of the chords. We can represent this as

$$\{(a; b; c); k\} = \{a + k; b + k; c + k\}$$

We need to determine the number of distinct orbits to determine the number of different triads we can make. To do this, we identify the elements of our group:

1. $k = 0$ (Identity Transformation)

All of these are fixed points because nothing is changed after the identity transformation, so $|x| = ({}^{12}C_3)$

2. $k = 4$

This will lead to a fixed point if and only if the following equation holds true

$$4\{a; b; c\} = \{a + 4; b + 4; c + 4\} = \{a; b; c\}$$

This results in four triples, so $|X^4| = 4$

3. $k = 8$

Using the same reasoning as above, we also have $|X^8| =$

4. These are the only possible fixed points that exist because in any d -tone system where we are selecting n -tuples of tones, the only value k that we can

have fixed points is when kn is a multiple of d . In this situation, we have a 12-tone system and we are selecting 3 tuples of tones. So, this means that the only possible fixed points is when $3k$ is a multiple of 12, so when $k = 0, 4, 8$.

Using Burnside's Lemma, we calculate that the number of distinct orbits, which represent the number of distinct triads, is equal to

$$\begin{aligned} 1/|G| \sum_{g \in G} |x^g| &= 1/12(x^0 + x^4 + x^8) \\ &= ({}^{12}C_3 + 4 + 4)/12 \\ &= 228/12 = 19 \end{aligned}$$

This represents the number of distinct triads for triples, but similar methods can be used to enumerate the different n -tuples tones as well.

Conclusion :-

We have discussed applications of Burnside Lemma and Polya Enumeration theorem in this project. We have noticed that we can only count the number of distinct colourings by Burnside Lemma and to know about their configuration we have to use Polya Enumeration theorem. Then we have described the Polya Enumeration theorem shortly and from its many fields of applications we have chosen Chemical Isomer Enumeration and Music theory Enumeration for discussion. Since in chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecules in space which are called isomers, we can use Polya Enumeration Theorem to enumerate these types of isomers. In music theory, Polya Enumeration theorem is used to identify patterns within chord sequences, in addition to counting the number of patterns in intervals and rhythms.

References

[1] Polya Enumeration Theorem :

https://en.wikipedia.org/wiki/P%C3%B3lya_enumeration_theorem

[2] Matias von Bell. Polya's Enumeration Theorem and its Applications. Dec, 2015.

- <https://helda.helsinki.fi/bitstream/handle/10138/159032/GraduTiivistelma.pdf?sequence=3>

[3] Harald Friertinger and Graz Voitsberg.

Enumeration in Music Theory

- <http://emis.math.tifr.res.in/journals/SLC/opapers/s26friert.pdf>

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE



PROJECT WORK

Topic :- Applications of Group Theory

MATHEMATICS DEPARTMENT

Submitted for partial fulfillment of the B.Sc. Degree in Mathematics

By **Gopal Samanta**

COLLEGE ROLL :- **308**

REGISTRATION NO :- **A01-1112-113-005-2019**

EXAMINATION ROLL:- **2022151095**

PAPER CODE :- **MTMA CC-XII**

SEMESTER :- **5 TH (UG)**

Supervised By :- Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENTS

I gratefully acknowledge our respected Principal Maharaja for giving us inspiration and motivation.

I am grateful to my advisor **DR. PRAVANJAN KUMAR RANA** Associate Professor, Department of Mathematics, Ramakrishna Mission Vivekananda Centenary College , Kolkata-700118 for his guidance on the related area of this project work and continuous support.

I am also very much thankful to our respected teachers , whose valuable teaching and research ideas have continuously motivated me. I am also thankful to all other respected staffmembers of our department.

Finally, my deepest admiration goes to my parents for their all-out support through out my life.

Gopal Samanta

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata-700118

Date:- 24/01/2022

Place:- Rahara

APPLICATION'S OF GROUP THEORY

1) ABSTRACT:-

Group Theory is one of the most important part of our daily life. Here we are going to introduce an idea how the group thorey help us in TIC-TAC-TOE Game, Symmetry & Barcode.

2)INTRODUCTION:-

To fully understand the math behind group theory one needs to take a look at the theory portion of the Group Theory topic or refer to one of the reference text listed at the bottom of this project. Never the less as Chemist the object the question we are examining is usually a molecule. Though we live in the 22nd century and much is known about the physical aspects that give rise to molecular and atomic properties. The number of high level calculations that need to be performed can be both time consuming and tedious. To most experimentalist this task is takes away time and is usually not the integral part of our work. When one thinks of group theory applications one doesn't necessarily associated it with everyday life or a simple toy like a Rubik's cube.

3) MY IDEA'S:-

● Maths Problem : Tic-Tac-Toe Game (Burnside's Lemma)::

If we want to know how many different ways are there to completely fill a noughts and cross grid, using four noughts and five crosses (Not including rotations and reflections of the board)---

×	×	0
0	0	×
×	0	×

Now the answer will be 23 i.e, there are 23 different ways to completely fill a noughts and crosses grid. There are a couple ways to solve this. But we can also solve it by Mathematician's ways i.e, **BURNSIDE'S LEMMA** .

We can also solve it by using rotations and reflections, but that will be very lengthy.



First of all, how can we fill 3×3 grids, using four noughts and five crosses = $\frac{9!}{4! \times 5!}$

$$=126$$

0 0 0 0

× × × × ×

We can use Burnside's Lemma to determine the required number .

Here we consider Eight Symmetries – Identity ,90° rotation, 180° rotation, 270° rotation and four reflection.

Burnside Lemma ::

$$\text{Total number of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

[the number of orbits is equal to the average number of fixed points.]

We can substitute the size of the group $|G|=8$

First we consider the fixed elements of the identity.

For identity, there are 126 grids that remains unchanged. So its fix size=126.

Now we consider the fix size for the 90° rotation. For 90° rotation there are only two grids that remain unchanged . So its fix size=2.

Simmilarlly, 180° and 270° rotation the fix size are 6 and 2 respectively.

For a rotation, either side of the reflection will have to look the same. Here we find 12 grids that remain unchanged.

So for each reflection the fix size=12

Total fixed size=126+2+6+2+12+12+12+12

=184.

By Burnside's Lemma number of orbits = $\frac{184}{8}$

= 23.

● Symmetry (In Chemistry)::

The dihedral group can be defined as the group of symmetries n-gon ,and such a geometric definition is easier to graso because it is very visual as opposed to an abstract definition. We learned that the dihedral group (D_n) was defined as

$$D_n = \{e, r^k, s, r^k s\} \text{ (k and n both integers) where}$$

- 1) The identity operation (e) causes no change.
- 2) The rotation operation r^k (also called proper rotation) where $k=\{1,n\}$ is a counterclockwise rotation of $k \frac{360^\circ}{n}$ about a rotation axis. Where $k=n$, $r^n = e$ (Since rotation of 360° is the identity operation

- 3) The reflection operation (σ) exchanges left & right, as if each point had moved perpendicularly through the plane to a position exactly as far from the plane as it started. If k is even, $k=2p$, $\sigma^{2p}=e$
- 4) A rotation-reflection operation (σ^k) (Sometimes called an improper rotation) requires a rotation of k ($360^\circ/n$) followed by reflection through a plane perpendicular to the axis of rotation.

In this section, we decided to look primarily at symmetry operations of simple linear molecules from geometric and group theoretical approach. I choose a basic linear molecule carbon dioxide (CO_2) which has the following molecule representations:

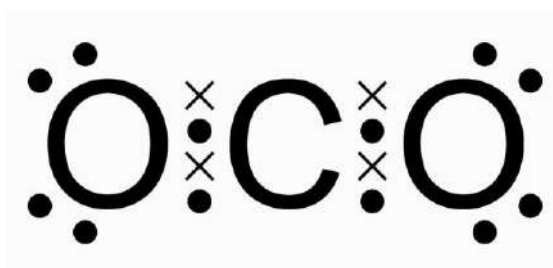


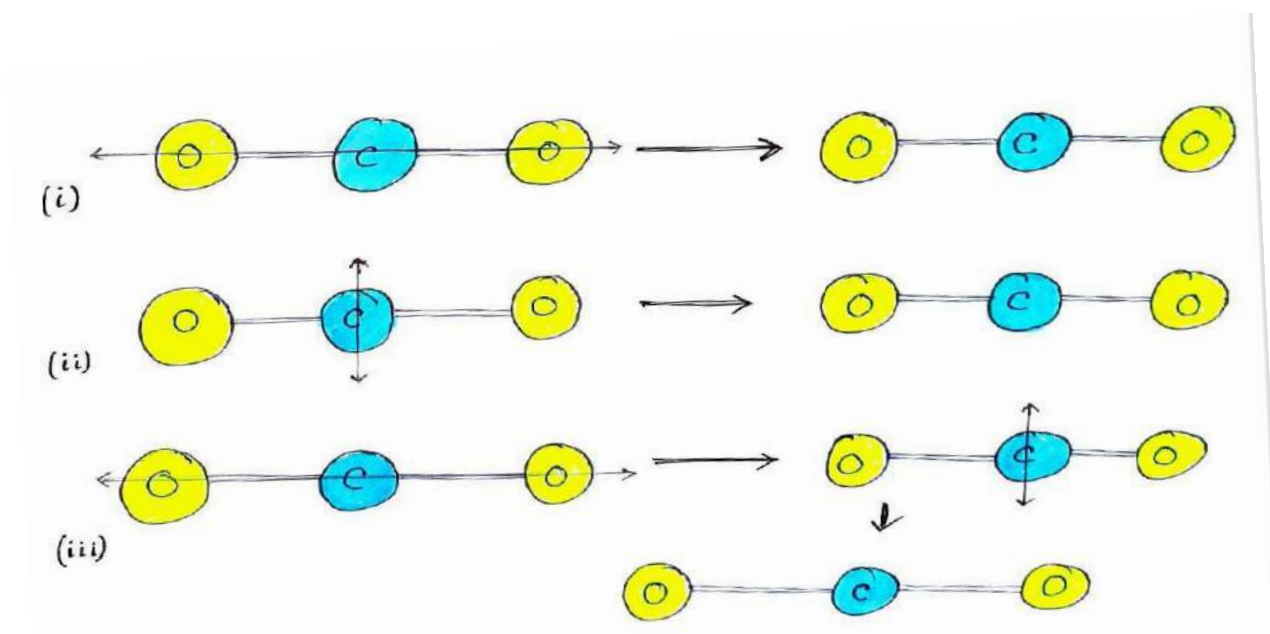
Figure-1



Figure-2

Observing figure-1 the Lewis structure of CO_2 . Oxygen atom has six valence electrons and carbon has four valence electrons and CO_2 is sp hybridized. So CO_2 is linear and planar structure. In this case to maximize distance, the atoms form a 180° angle with the centralized atom as a vertex. Looking at Figure-2 it is very easy to see the symmetry operations for CO_2 .

- (1) A rotation around a central horizontal C_∞ axis
- (2) A reflection about a central and then
- (3) a composition of 1 & 2 or a rotation followed by a reflection. The identity operation (e) is also a symmetry operation.



Now, if we see in the structure Boron Trifluoride (BF_3) then 24 valence electrons are there and its an SP^2 hybridization. So, its Triangle planner i.e, it's same as D_3 . So we can apply rotation & reflection

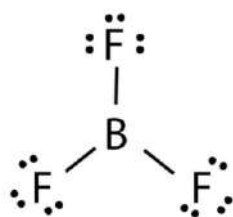


Figure :- BF_3

And when we see in the structure Xenon Tetrafluoride and it's (XeF_4), has 36 valence electrons and SP^3d^2 hybridization and it's square planner structure. i.e, it's same as D_4 i.e, we can take the operation rotation 90° , rotation 180° , rotation 270° , reflection horizontally, reflection vertically, reflection in main main diagonally and reflection with respect to another diagonal.

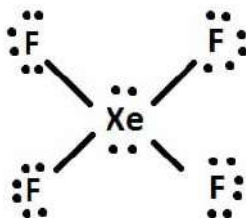


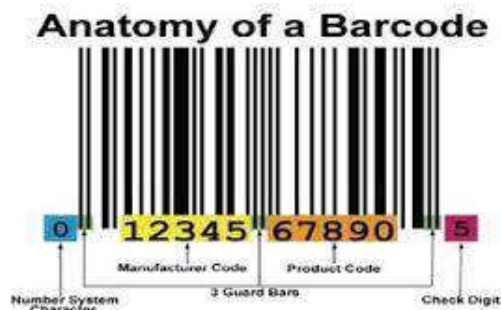
Figure :- XeF_4

● Barcode::

We also know as Universal Product Code (UPC). A UPC-A identification number has 12- digits. The first six digits identify manufacture, the next five digits identify the product and 1st is a check An item with UPC identification number

$$(a_1, a_2, \dots, a_{12})(3, 1, 3, 1, \dots, 3, 1) \bmod 10 = 0.$$

Now suppose a single error is made in entering the the number in computer , it won't satisfy the condition.



::Conclusion::

In this project, we want to discuss some applications of group theory. We know the theory portion, but if don't know the application of that then it's like 'I have a car, but I don't know the drive'. So when we read dihedral group then from that portion we want to discuss symmetrical structure of some chemical compounds, i.e, from here we can conclude that in chemistry we can see application of group theory. After that when we want to solve in how many ways are there obviously in different ways to complete the Tic-Tac-Toe game by four noughts and five crosses, then we can solve it by rotation and reflection of the board and Interchanging of grids. Then we get the answer 23 .But it's very lengthy process, but if we solve it by group action mainly by Burnside Lemma, we can easily solve this. So from here we can conclude that in game there are application of group theory.

::Reference::

- 1) Contemporary Abstract Algebra; Joseph A. Gallian
- 2) Fundamental of Abstract Algebra; D.S.Malik,, John N. Mordeson,, M.K.Sen.
- 3) Chemistry (Inorganic & Organic); Dr.Rabindranath Maiti, Nemai Tewari, Sabithabrata Roy.

College Name: Ramakrishna Mission Vivekananda Centenary College

Name: Anischay Pal

Reg. No: A01-1112-113-006-2019

Exam Roll No: 2022151096

College Roll No: 309

Project Topic: Todd-Coxeter Algorithm

Supervised by: Pravanjan Kumar Rana

Acknowledgement

I would like to express my special thanks of gratitude to my advisor, Prof. Pravanjan Kumar Rana, who introduced me to the wonderful project work. I would also like to thank him for the guidance, patience, and help and for contributing from his abundance experience, knowledge and wisdom. It was an honour for me to get a glimpse to his world and way of thinking. My friends Sreyan Jha and Partha Das also helped me to do this project work, I am also thankful to them.

Content

<u>Sl No.</u>	<u>Subject</u>	<u>Page No.</u>
01.	Introduction	4
02.	Todd-Coxeter Algorithm	4-6
03.	Example	7-13
04.	Implementation	13-15
05.	Application	15-16
06.	Conclusion	17
07.	References	17

Introduction:

In group theory, the **Todd–Coxeter algorithm**, created by J. A. Todd and H. S. M. Coxeter in 1936, is an algorithm for solving the coset enumeration problem. Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm is a strategy for writing down the set of left cosets of H in G together with the action of G on the set.

Todd–Coxeter Algorithm:

Let G be the finitely presented group

$$G := \langle g_1, g_2, \dots, g_n \mid r_1(g_1, g_1, g_2, \dots, g_n) = e, \dots, r_m(g_1, g_1, g_2, \dots, g_n) = e \rangle$$

or shorter $G := \langle E \mid R \rangle$ where $E := \{g_1, g_2, \dots, g_n\}$ and $R := \{r_i(g_1, g_1, g_2, \dots, g_n) \mid i = 1, 2, \dots, m\}$ where each relator $r_i(g_1, g_1, g_2, \dots, g_n)$ is a word in g_1, g_2, \dots, g_n and e is the identity of G , and let H be the subgroup of G generated by the set S of words,

$$S := \{s_1(g_1, g_1, g_2, \dots, g_n), \dots, s_p(g_1, g_1, g_2, \dots, g_n)\}$$

that is, $H := \langle S \rangle$.

The algorithm is based on two simple facts:

1. If $s \in S$, then $Hs = H$.
2. If $r(g_1, \dots, g_n)$ is a relator, then for any coset Hx , $x \in G$ we have $Hxr(g_1, \dots, g_n) = Hx$. So if $r(g_1, \dots, g_n) = g_{i1} \dots g_{it}$ where each g_{ij} is a

generator or an inverse of a generator, then: $H_0 := Hx$, $H_1 := H_{0g_{i1}}$, $H_2 := H_{1g_{i2}}$, \dots , $H_j := H_{j-1g_{ij}}$ is defined, then $H_t = H_0$.

Now, for the procedure itself: for each word that generates the subgroup H we maintain a one-line table, called a subgroup table. The row is labelled as 1 for the coset H itself. The columns are labelled by the factors of the generator of the word. That is, if $s_j = g_{i1} \dots g_{ik}$ is a generator of H , then we have $k + 1$ columns.

Subgroup Table

g_{i1}	g_{i2}	\dots	g_{ik}
1			1

If we look at the table as a matrix of order $1 \times (k + 1)$, then the entry $(1, g_{ij})$ in the table, if defined, is the number of the coset we get from the multiplication $1 \cdot g_{i1} \dots g_{ij}$.

For each relator, $r (g_1, \dots, g_n)$ we have a relation table. Relation tables will give us information in case two cosets which have numbered differently are the same. If a relation acts on two cosets in exactly the same way, then these cosets must be identical. The rows of the relation tables are labelled with the numbering we defined for the cosets. Similarly to the subgroup table, given a relator $r_i = g_{i1} \dots g_{ik}$, we have $k + 1$ columns.

Relation table for $r_i = g_{i1} \dots g_{ik}$

$g_{i1}g_{i2} \dots g_{ik}$		
	1	1
	2	2
	.	.
	.	.
	.	.
	t	t
	.	.
	.	.

As in the subgroup table, the entry (n, g_{ij}) if defined, is the coset we get from the multiplication $n \cdot g_{i1} \cdot g_{i2} \cdots g_{ij}$. Since we know that $r_i = g_{i1} \cdots g_{ik} = e$, we get that $Hx_{r_i} = Hx$. So the entry (n, g_{ik}) is n .

Finally, we would like to have a table that keeps track for us on the result of multiplications. This table is the coset table. The rows will be labelled with the numbers of the cosets, and the columns will be labelled by the generators of G and their inverses (unless a generator is an involution). The entry (n, g_i) , if defined, is $n \cdot g_i$ for the coset n and the generator g_i .

When the last entry in a row of a relation table or a subgroup table is filled in, we get an extra piece of information, in the form of $n \cdot g = l$, for some cosets n, l and a generator g . This extra piece of information is called a deduction. When getting a deduction we can face three situations:

- (i) The entries (n, g) and (l, g^{-1}) are still empty. In this case, we just fill the number l in the entry (n, g) and the number n in the entry (l, g^{-1}) . We also insert this information into all other relevant places in the other tables.
- (ii) The entry (n, g) is already filled with the number l . In this case, the deduction brings no new information.
- (iii) At least one of the entries (n, g) or (l, g^{-1}) in the coset tables is filled with a number different from l or n , respectively. In this case, we conclude that we have two different numbers to the same coset. This phenomenon is called a coincidence. When a coincidence is found, we replace both numbers by the smaller one in all places they occur.

The process terminates when all the entries of the coset, relation and subgroup tables are filled.

We would like to give a detailed example of the Todd-Coxeter Algorithm for the group S_4 , using generators and relations, as follows:

$G := \langle a, b, c \mid a^2 = b^2 = c^2 = e, (ab)^3 = e, (bc)^3 = e, (ac)^2 = e \rangle$

and taking the subgroup

$H := \langle a, b \rangle$.

We have to use some useful proposition

- (i) The set of transpositions $\{(1, k) \mid 1 \leq k \leq n\}$ generate S_n , for $n \geq 2$
- (ii) The set of transpositions $\{(12), (23), \dots, (n-1, n)\}$ generate S_n , for $n \geq 2$.

First, we define three cosets and try to fill in the tables. Then we will be able to see whether we need to define more cosets in order to complete the tables, or not.

We define:

$1 := H, 2 := 1c, 3 := 2b$.

The subgroup tables are already closed, and as expected, we did not gain any additional information from them.

Subgroup Tables

<u>a</u>		<u>b</u>	
1	1	1	1

However, from the definitions and the relations in the group G , we can immediately derive the following: $2c = 1$, $3b = 2$, as b and c are of order 2. We should note that there are a few possible ways to fill in the tables. One can start from the left or from the right and then can continue using any combination of them. Nevertheless, eventually one arrives at the same result.

Now, let us start filling in the coset and relation tables:

Coset table

	a	b	c
1	1	1	2
2	2	3	1
3		2	3

Relation tables for $a^2 = e$, $b^2 = e$, $c^2 = e$

<u>a a</u>			<u>b b</u>			<u>c c</u>		
1	1	1	1	1	1	1	2	1
2	2	2	2	3	2	2	1	2
3		3	3	2	3	3	3	3

Relation table for $(ab)^3 = e$

<u>a b</u>		<u>a b</u>		<u>a b</u>	
1	1	1	1	1	1
2	2	3		3	2
3		3	2	2	3

Relation table for $(ac)^2 = e$

	a	c	a	c
1	1	<u>2</u>	<u>2</u>	1
2	2	1	1	2
3	3		3	3

Relation table for $(bc)^3 = e$

b	c	b	c	b	c	
1	1	2	3	3	2	1
2	<u>3</u>	<u>3</u>	2	1	1	2
3	2	1	1	2	3	3

In the process of filling in the tables we have received the following deductions, $2a = 2$, $3c = 3$, which we have underlined in the table, in the place we got them.

Now, one can define one more coset and continue, or to define a few more at once. As we shall see, it is enough to define only one more coset, namely, $4 := 3a$ to complete all the tables. However, since we would like to demonstrate the notion of "coincidences" we shall take the latter approach: we shall define three more cosets at once: $4 := 3a$, $5 := 4b$, $6 := 4c$. Continuing filling in the tables gives

	a	b	a	b	a	b
1	1	1	1	1	1	1
2	2	3	<u>4*</u>	<u>4*</u>	3	2
3	4	<u>5*</u>	<u>3*</u>	2	2	3
4	3	2	2	3	5	4
5	3	2	2	3	4	5
6	3	2	2	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 ₅	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we receive the following deductions: $4b = 4$ and $5a = 3$. However, as we see in the coset table, the place of $4b$ is already filled with 5. Therefore, we get a coincidence: cosets 4 and 5 are the same coset of H in the group G . Similarly, the place of $3a$ is already filled with 4 in the coset table, which means, as have already discovered, that 4 and 5 are the same coset. We note that coincidences are marked in the tables with asterisk(*). Equipped with the previous information, let us continue to the other relation tables.

	a	c	a	c
1	1	2	2	1
2	2	1	1	2
3	4	<u>6*</u>	<u>3*</u>	3
4	3	3	4	4
5	3	3	4	5
6	3	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 _{5,6}	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we get the information that $6a = 3$ or, equivalently, $3a = 6$. This yields another coincidence: this time we get that cosets 4 and 6 are the same cosets of H in G . So, from the last two coincidences we have $4 = 5 = 6$. These coincidences yield full information about the multiplication of all the elements we have, or in other words, we filled in the whole coset table, and thus can fill in the rest of the tables completely. As we said in the description of the algorithm, we take the smallest integer in a coincidence to represent the equal cosets.

	a	b	c
1	1	1	2
2	2	3	1
3	$4_{5,6}$	2	3
4	3	5_4	6_4
5	3	4	4
6	3	4	4

<u> a a </u>			<u> b b </u>			<u> c c </u>		
1	1	1	1	1	1	1	2	1
2	2	2	2	3	2	2	1	2
3	4	3	3	2	3	3	3	3
4	3	4	4	5	4	4	6	4
5	3	5	5	4	5	5	4	5
6	3	6	6	4	6	6	4	6

<u> b c b c b c </u>						
1	1	2	3	3	2	1
2	3	3	2	1	1	2
3	2	1	1	2	3 3	
4	4	4	4	4	4	4
5	4	4	4	4	4	5

6 4 4 4 4 4 6

Eventually, we receive four different cosets of H in G , which are 1,2,3 and 4. This means that $[G : H] = 4$, and since $|H| \leq 6$ then we get an upper bound to the order of G , that is, $|G| \leq 24$. On the other hand, we know that the three transpositions (12),(23),(34), of which the generators of G act on the cosets 1,2,3 and 4, generate S_4 and we get an epimorphism from G onto S_4 (or equivalently, S_4 is a homomorphic image of G), which means that $|G| \geq 24$. All in all, we get that $|G| = 24$ and thus $G \cong S_4$.

Implementation

Now we give a concrete implementation of the algorithm in Python. For simplicity, we will just compute $S_3/\langle b \rangle$ with the presentation $\langle a, b | a^3, b^2, abab \rangle$

The main data structures are

```
idents = []
neighbors = []
to_visit = 0

ngens = 2
rels = [
    (1, 0), # a^-1a
    (3, 2), # b^-1b
    (0, 0, 0), # a^3
    (2, 2), # b^2
    (0, 2, 0, 2) # abab
]
hgens = [
    (2,), # b
]

def find(c):
    c2 = idents[c]
    if c == c2:
        return c
    else:
        c2 = find(c2)
        idents[c] = c2
        return c2
```

```

def new():
    c = len(idents)
    idents.append(c)
    neighbors.append((2*ngens)*[None])
    return c

def unify(c1, c2):
    c1 = find(c1)
    c2 = find(c2)
    if c1 == c2:
        return
    c1, c2 = min(c1, c2), max(c1, c2)
    idents[c2] = c1
    for d in range(2*ngens):
        n1 = neighbors[c1][d]
        n2 = neighbors[c2][d]
        if n1 == None:
            neighbors[c1][d] = n2
        elif n2 != None:
            unify(n1, n2)

def follow(c, d):
    c = find(c)
    ns = neighbors[c]
    if ns[d] == None:
        ns[d] = new()
    return find(ns[d])

def followp(c, ds):
    c = find(c)
    for d in reversed(ds):
        c = follow(c, d)
    return c

start = new()

for hgen in hgens:
    unify(followp(start, hgen), start)

while to_visit < len(idents):
    c = find(to_visit)
    if c == to_visit:
        for rel in rels:
            unify(followp(c, rel), c)
    to_visit += 1

print ("done")

```

```

cosets = [c for i, c in enumerate(idents) if i == c]

perms = [[cosets.index(follow(c, 2*d)) for i, c in enumerate(cosets)]
          for d in range(ngens)]

def cycle(perm):
    parts = []
    for i in range(len(perm)):
        part = [str(i+1)]
        k = perm[i]
        while k != i:
            if k < i: break
            part.append(str(k+1))
            k = perm[k]
        else:
            parts.append(" ".join(part))
    return "("+"+"").join(parts)+"")"

for d in range(ngens):
    print ("g%d ="%d, cycle(perms[d]))

```

For these particular relations, the output is

```

done
g0 = (1 2 3)
g1 = (1)(2 3)

```

Application:

By using this algorithm, Coxeter and Todd showed that certain systems of relations between generators of known groups are complete, that is constitute systems of defining relations. If the order of a group G is relatively small and the subgroup H is known to be uncomplicated, then the algorithm can be carried out by hand and gives a reasonable description of the group G . It is a systematic procedure for enumerating the cosets of a subgroup of finite index in a group given by generators and relations.

The algorithm has been an important component in most computer programs to date dealing with symbolic calculation in algebra.

We use programmes for the Todd-Coxeter coset enumeration algorithm and the modified Todd-Coxeter coset enumeration algorithm to investigate a class of generalised Fibonacci groups. In particular we use these techniques to discover a finite non-metacyclic Fibonacci group.

There are a number of things one can deduce from the result of the algorithm.

- Of course, if it terminates, we deduce $[G:H]$ is finite (and know what it equals).
- A permutation representation of G/H , given by a permutation of G/H for each generator of G .
- Whether H is a normal subgroup. This can be determined by seeing whether each generator's permutation is an element of $\text{Aut}(G/H)$, since then $\text{Aut}(G/H) = G/H$, implying H is normal.
- An algorithm for the word problem for the group. Given two words, follow the graph from the basepoint to see whether they end on the same vertex.
- The algorithm also helps to compute the data of a uniform polytope.

Conclusion:

The Todd–Coxeter algorithm can be applied to infinite groups and is known to terminate in a finite number of steps, provided that the index of H in G is finite. On the other hand, for a general pair consisting of a group presentation and a subgroup, its running time is not bounded by any computable function of the index of the subgroup and the size of the input data.

References:

- .Brown, Ken. *The Todd-Coxeter procedure*.
- Coxeter, H. S. M.; Moser, W. O. J. (1980). *Generators and Relations for Discrete Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 14 (4th ed.). Springer-Verlag 1980. ISBN 3-540-09212-9. MR 0562913.
- Seress, Ákos (1997). "An introduction to computational group theory" (PDF). Notices of the American Mathematical Society. 44 (6): 671–679. MR 1452069.

**RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE**



PROJECT WORK

Topic :- Applications of Group Theory

MATHEMATICS DEPARTMENT

Submitted for partial fulfillment of the B.Sc. Degree in Mathematics

By Ujjal Pattanayek

COLLEGE ROLL :- 314

REGISTRATION NO :- A01-1112-113-008-2019

EXAMINATION ROLL:- 2022151097

PAPER CODE :- MTMA CC-XII

SEMESTER :- 5 TH (UG)

Supervised By :- Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENTS

I gratefully acknowledge our respected Principal Maharaja for giving us inspiration and motivation.

I am grateful to my advisor **DR. PRAVANJAN KUMAR RANA** Associate Professor, Department of Mathematics, Ramakrishna Mission Vivekananda Centenary College , Kolkata-700118 for his guidance on the related area of this project work and continuous support.

I am also very much thankful to our respected teachers , whose valuable teaching and research ideas have continuously motivated me. I am also thankful to all other respected staffmembers of our department.

Finally, my deepest admiration goes to my parents for their all-out support through out my life.

Ujjal Pattanayek

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata-700118

Date:- 24/01/2022

Place:- Rahara

APPLICATION'S OF GROUP THEORY

1) ABSTRACT:-

Group Theory is one of the most important part of our daily life. Here we are going to introduce an idea how the group thorey help us in TIC-TAC-TOE Game, Symmetry & Barcode.

2)INTRODUCTION:-

To fully understand the math behind group theory one needs to take a look at the theory portion of the Group Theory topic or refer to one of the reference text listed at the bottom of this project. Never the less as Chemist the object the question we are examining is usually a molecule. Though we live in the 22nd century and much is known about the physical aspects that give rise to molecular and atomic properties. The number of high level calculations that need to be performed can be both time consuming and tedious. To most experimentalist this task is takes away time and is usually not the integral part of our work. When one thinks of group theory applications one doesn't necessarily associated it with everyday life or a simple toy like a Rubik's cube.

3) MY IDEA'S:-

● Maths Problem : Tic-Tac-Toe Game (Burnside's Lemma)::

If we want to know how many different ways are there to completely fill a noughts and cross grid, using four noughts and five crosses (Not including rotations and reflections of the board)---

×	×	0
0	0	×
×	0	×

Now the answer will be 23 i.e, there are 23 different ways to completely fill a noughts and crosses grid. There are a couple ways to solve this. But we can also solve it by Mathematician's ways i.e, **BURNSIDE'S LEMMA** .

We can also solve it by using rotations and reflections, but that will be very lengthy.



First of all, how can we fill 3×3 grids, using four noughts and five crosses = $\frac{9!}{4! \times 5!}$

$$=126$$

0 0 0 0

× × × × ×

We can use Burnside's Lemma to determine the required number .

Here we consider Eight Symmetries – Identity ,90° rotation, 180° rotation, 270° rotation and four reflection.

Burnside Lemma ::

$$\text{Total number of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

[the number of orbits is equal to the average number of fixed points.]

We can substitute the size of the group $|G|=8$

First we consider the fixed elements of the identity.

For identity, there are 126 grids that remains unchanged. So its fix size=126.

Now we consider the fix size for the 90° rotation. For 90° rotation there are only two grids that remain unchanged . So its fix size=2.

Similarly, 180° and 270° rotation the fix size are 6 and 2 respectively.

For a rotation, either side of the reflection will have to look the same. Here we find 12 grids that remain unchanged.

So for each reflection the fix size=12

$$\begin{aligned} \text{Total fixed size} &= 126 + 2 + 6 + 2 + 12 + 12 + 12 + 12 \\ &= 184. \end{aligned}$$

$$\begin{aligned} \text{By Burnside's Lemma number of orbits} &= \frac{184}{8} \\ &= 23. \end{aligned}$$

● Symmetry (In Chemistry)::

The dihedral group can be defined as the group of symmetries n-gon ,and such a geometric definition is easier to grasp because it is very visual as opposed to an abstract definition. We learned that the dihedral group (D_n) was defined as

$$D_n = \{e, r^k, s, r^k s\} \text{ (} k \text{ and } n \text{ both integers) where}$$

- 1) The identity operation (e) causes no change.
- 2) The rotation operation r^k (also called proper rotation) where $k=\{1,n\}$ is a counterclockwise rotation of $k \cdot 360^\circ/n$ about a rotation axis. Where $k=n$, $r^n = e$ (Since rotation of 360° is the identity operation)

- 3) The reflection operation (σ) exchanges left & right, as if each point had moved perpendicularly through the plane to a position exactly as far from the plane as it started. If k is even, $k=2p$, $\sigma^{2p}=e$
- 4) A rotation-reflection operation (σ^k) (Sometimes called an improper rotation) requires a rotation of k ($360^\circ/n$) followed by reflection through a plane perpendicular to the axis of rotation.

In this section, we decided to look primarily at symmetry operations of simple linear molecules from geometric and group theoretical approach. I choose a basic linear molecule carbon dioxide (CO_2) which has the following molecule representations:

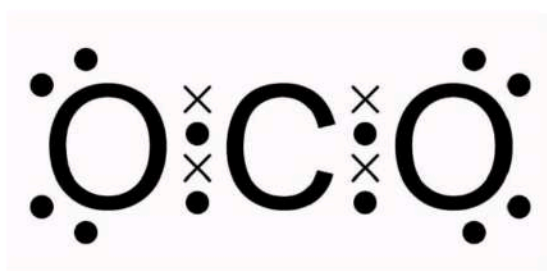


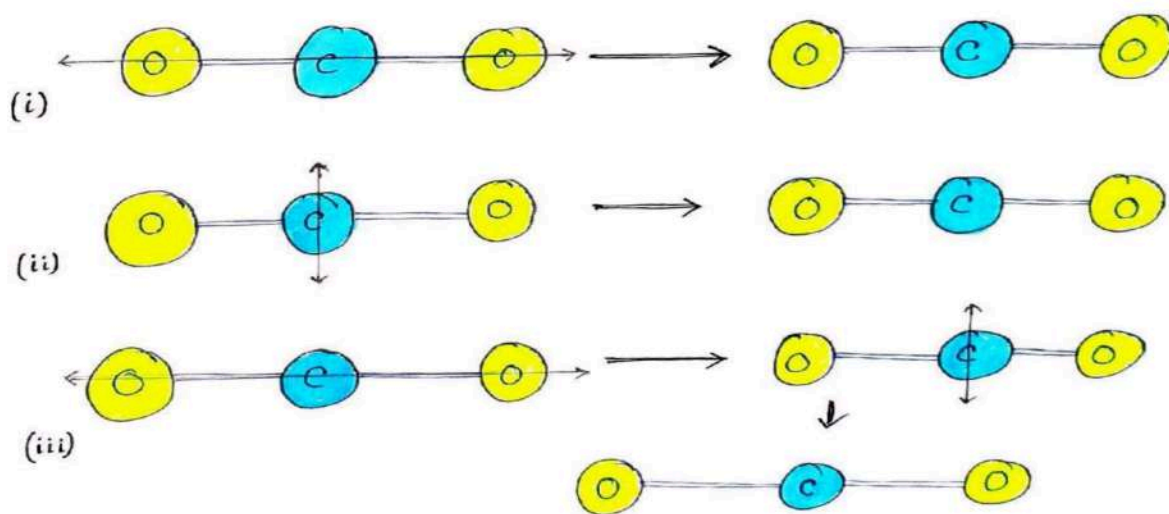
Figure-1



Figure-2

Observing figure-1 the Lewis structure of CO_2 . Oxygen atom has six valence electrons and carbon has four valence electrons and CO_2 is sp hybridized. So CO_2 is linear and planar structure. In this case to maximize distance, the atoms form a 180° angle with the centralized atom as a vertex. Looking at Figure-2 it is very easy to see the symmetry operations for CO_2 .

- (1) A rotation around a central horizontal C_∞ axis
- (2) A reflection about a central and then
- (3) a composition of 1 & 2 or a rotation followed by a reflection. The identity operation (e) is also a symmetry operation.



Now, if we see in the structure Boron Trifluoride (BF_3) then 24 valence electrons are there and its an SP^2 hybridization. So, its Triangle planner i.e, it's same as D_3 . So we can apply rotation & reflection

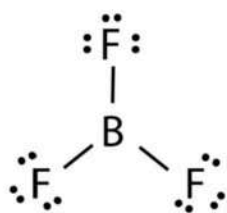


Figure :- BF_3

And when we see in the structure Xenon Tetrafluoride and it's (XeF_4), has 36 valence electrons and SP^3d^2 hybridization and it's square planner structure. i.e, it's same as D_4 i.e, we can take the operation rotation 90° , rotation 180° , rotation 270° , reflection horizontally, reflection vertically, reflection in main main diagonally and reflection with respect to another diagonal.

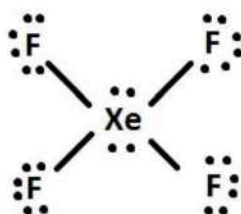


Figure :- XeF_4

● Barcode::

We also know as Universal Product Code (UPC). A UPC-A identification number has 12- digits. The first six digits identify manufacture, the next five digits identify the product and 1st is a check An item with UPC identification number $(a_1, a_2, \dots, a_{12})$ $(3, 1, 3, 1, \dots, 3, 1) \bmod 10 = 0$.

Now suppose a single error is made in entering the the number in computer , it won't satisfy the condition.



::Conclusion::

In this project, we want to discuss some applications of group theory. We know the theory portion, but if don't know the application of that then it's like 'I have a car, but I don't know the drive'. So when we read dihedral group then from that portion we want to discuss symmetrical structure of some chemical compounds, i.e, from here we can conclude that in chemistry we can see application of group theory. After that when we want to solve in how many ways are there obviously in different ways to complete the Tic-Tac-Toe game by four noughts and five crosses, then we can solve it by rotation and reflection of the board and Interchanging of grids. Then we get the answer 23 .But it's very lengthy process, but if we solve it by group action mainly by Burnside Lemma, we can easily solve this. So from here we can conclude that in game there are application of group theory.

::Reference::

- 1) Contemporary Abstract Algebra; Joseph A. Gallian
- 2) Fundamental of Abstract Algebra; D.S.Malik,, John N. Mordeson,, M.K.Sen.
- 3) Chemistry (Inorganic & Organic); Dr.Rabindranath Maiti, Nemai Tewari, Sabithabrata Roy.

RKMVCC RAHARA

Department of Mathematics

Semester: 5th

Core Course-XII

Group Theory-II

Project by:

Name- Soumyadeep Sarkar

Exam Roll Number-2022151098

Registration Number: A01-1122-113-009-2019

Supervised by:

Dr. Prabanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and my special gratitude to **Dr. Prabanjan kumar Rana, head of the department mathematics of RKMVCC Rahara**, who gave me a golden opportunity to do this project and also provided support in completing my project work.

I would also like to extend my gratitude to my friend Ritoprovo Roy, who helped me by sketching the drawings for my project.

TOPIC

Geometry of Orbits in Three Dimensional Sphere

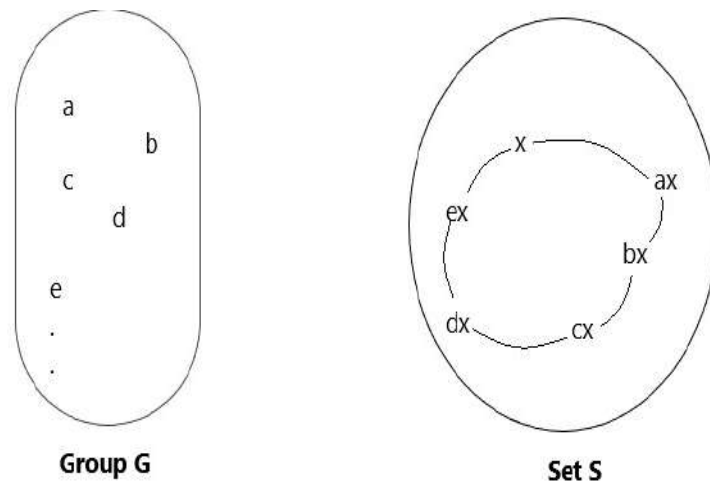
1. Abstract:

In this context we discussed geometry of orbits in light of three dimensional systems especially in a Sphere. Here we consider the group G as $(\mathbb{R}, +)$ and the set S as \mathbb{R}^2 . When S is a G set, we denote the group action by $\varphi: G \times S \rightarrow S$. Here the orbits orient themselves as a plane in three dimensional geometry containing three axes "X", "Y" & "Z" .

2. Introduction:

Let, G be any group whose elements are of the form $\{a, b, c, d, \dots e\}$. Also let S be a nonempty set & $x \in S$.

Keeping the element x fixed, we take all the elements of the form gx where $g \in G$ from the set S .



The set that contains elements of the form gx where $g \in G$, where x is a fixed element, is called the Orbit of x .

2.1 Definition of orbit:

Let, G be a group, acting on a non-empty set S . If $x \in S$, then the trajectory $\{\varphi(g, x): g \in G\}$ of the point x is called the orbit of the point x . It is denoted by O_x or by $[x]$.

2.2. Definition respect to equivalence relation:

Let, G be a group, acting on a non-empty set S . Now we define a relation ' \sim ' on S by $a \sim b \Leftrightarrow ga = b$ for some $g \in G$ & $\forall a, b \in S$. Then the relation ' \sim ' is an equivalence relation.

- The equivalence classes determined by the equivalence relation ' \sim ' are called the Orbits of G on S .

3. Concept of geometry of orbits:

For ease of understanding we can imagine the universe as a group. Then we can observe that every planet has own Orbit. We have the orbits never intersects with each other and they follow their own path. Each and every orbit has their different pattern of different shapes. We will discuss this in this context.

EXAMPLE-3.1: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x + t, y) \forall t \in G \ (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

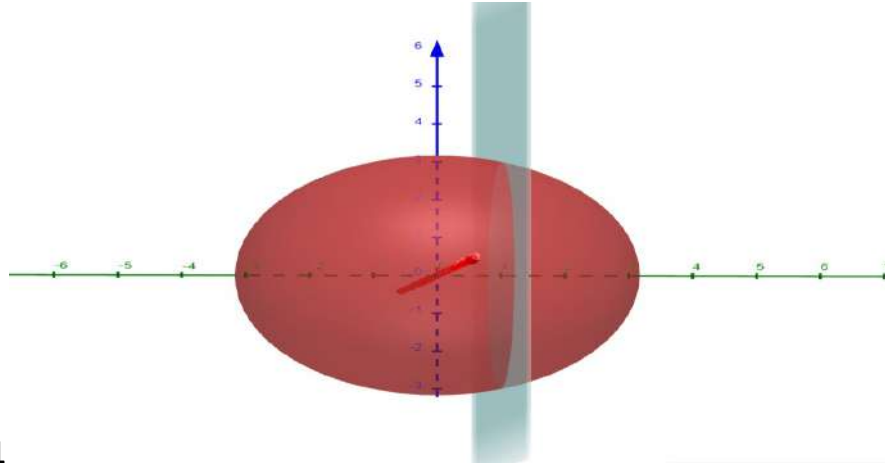
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), 1: t \in \mathbb{R}\}$$

$$\{(x, 1): x \in \mathbb{R}\}; \text{ where } (1 + t) = x$$

For this case the Y coordinate is always 1

i.e. horizontal line parallel to X axis, above the origin



Picture-1

Blue line= X axis

Green line= Y axis

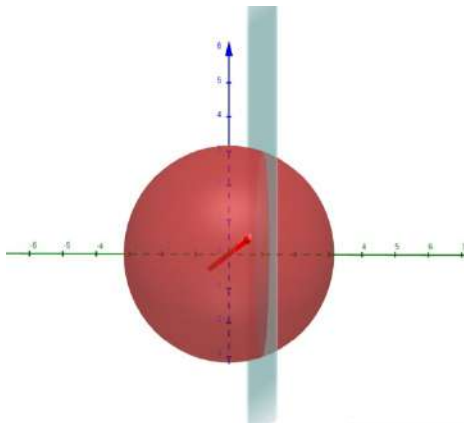
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), b: t \in \mathbb{R}\}$
 $\{(x, b): x \in \mathbb{R}\};$ where $(a + t) = x$

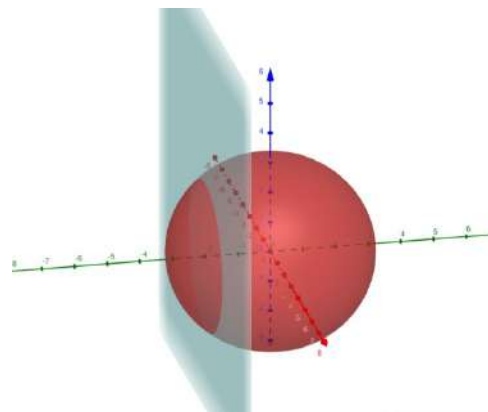
For this case Y coordinate is always b

When $b > 0$, the line is above origin, parallel to X axis

When $b < 0$, the line is below origin, parallel to X axis.



Picture-2



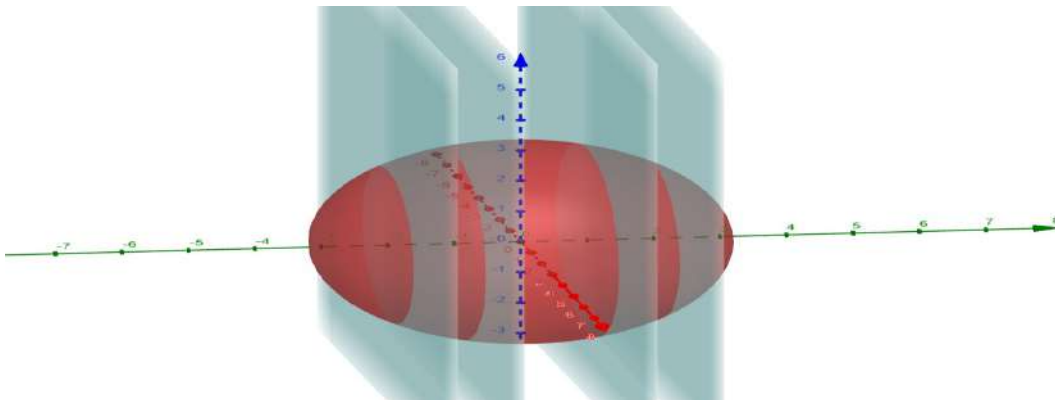
Picture-3

Blue line= X axis

Green line= Y axis

Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-4

Blue line= X axis

Green line= Y axis

Red line= Z axis

EXAMPLE-3.2: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x, y + t) \forall t \in G \text{ and } (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

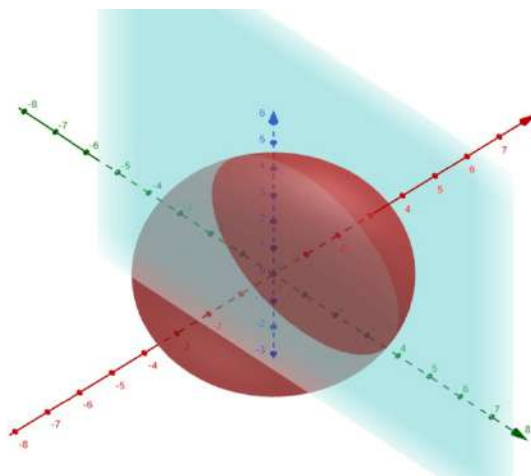
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{1, (1 + t): t \in \mathbb{R}\}$$

$$\{(1, y): x \in \mathbb{R}\}; \text{ where } (1 + t) = y$$

For this case the X coordinate is always 1

i.e. horizontal line parallel to Y axis.



Picture-5

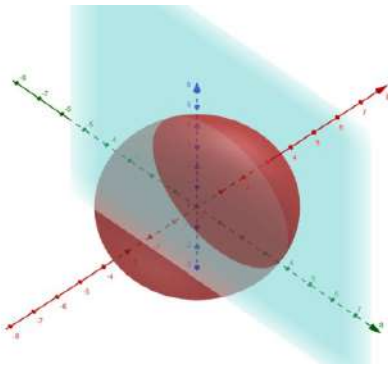
Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{a, (t + b): t \in \mathbb{R}\}$
 $\{(a, y): y \in \mathbb{R}\}$; where $(b + t) = y$

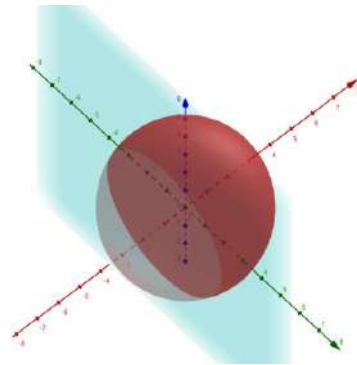
For this case X coordinate is always a

When $a > 0$, the line lies on right side of the origin, parallel to Y axis

When $a < 0$, the line lies on left side of the origin, parallel to Y axis.



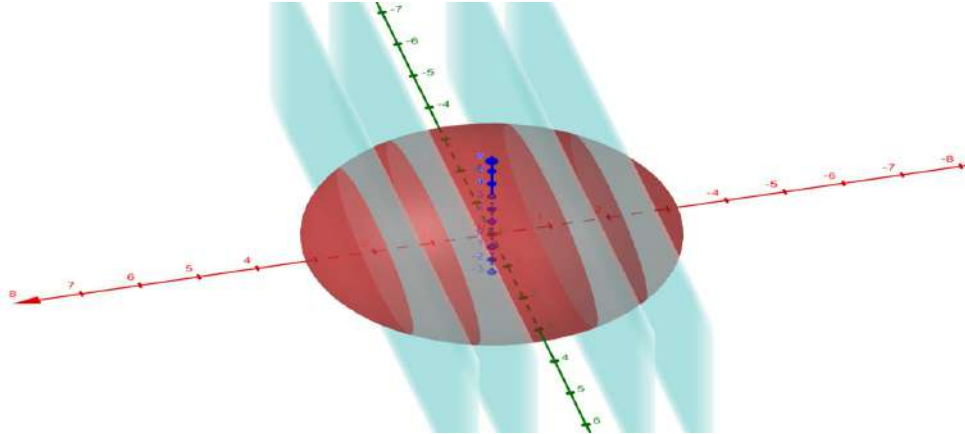
Picture-6



Picture-7

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-8

Blue line= X axis
Green line= Y axis
Red line= Z axis

EXAMPLE-3.3: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map $\alpha: G * S \rightarrow S$ by $\alpha\{t, (x, y)\} = t. (x, y) := (x + t, y + t) \forall t \in G$ and $(x, y) \in \mathbb{R}^2$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

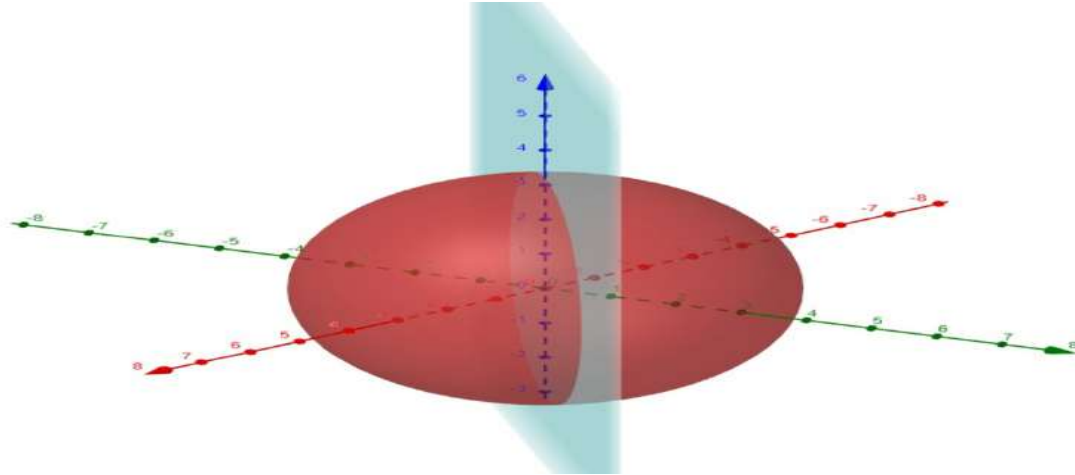
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), (1 + t): t \in \mathbb{R}\}$$

$$\{(x, x): x \in \mathbb{R}\} ; \text{ where } (1 + t) = x$$

As x is a arbitrary real number and $y = x$ so it passes through the origin and slope 1.

The picture is given below,



Picture-9

Blue line=X axis
Green line=Y axis
Red line=Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), (t + b): t \in \mathbb{R}\}$

As $t \in \mathbb{R}$ so take two different values of t namely $t = 0$ and $t = 1$

Then we have the required line passes through the points (a, b) & $(a + 1, b + 1)$

Equation of the line will be: $\frac{y - y_2}{y_1 - y_2} = \frac{x - x_2}{x_1 - x_2}$

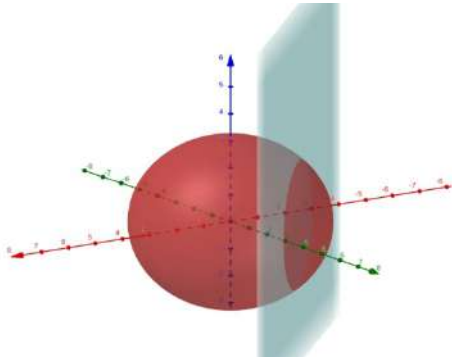
$$\text{Or, } \frac{y - b}{b + 1 - b} = \frac{x - a}{a + 1 - a}$$

$$\text{Or, } x - y = (a - b)$$

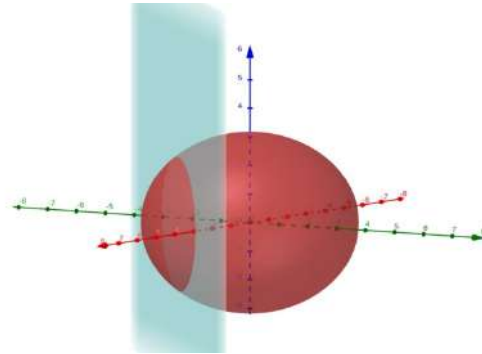
$$\text{Or, } y = x - (a - b)$$

This shows that the slope is 1 but the intercept is non zero.

When $a > b$, the intercept is negative and When $a < b$, the intercept is positive.



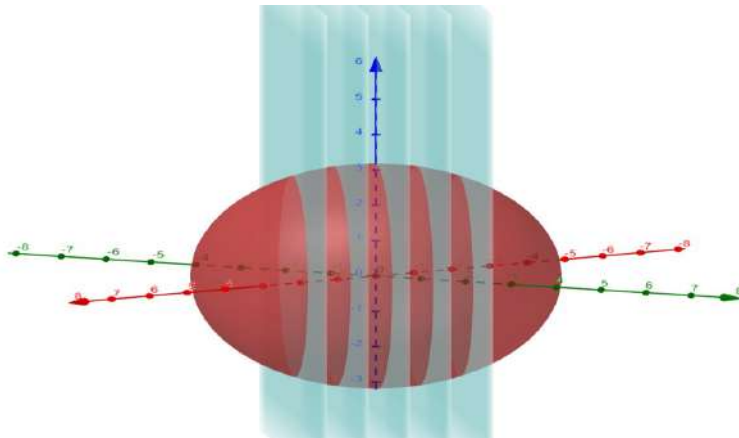
Picture-10



Picture-11

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-12

Blue line= X axis
Green line= Y axis
Red line= Z axis

4. Conclusion

Let G be a group and S be a non empty set. Suppose $x \in S$. Then, we wish to find the notation for Orbit of x .

Orbit of x , denoted by

$$\begin{aligned}[x] &= \{g \cdot x : g \in G\} \\ &= \{y \in S : y = g \cdot x \text{ for some } g \in G\} \\ &= \{y \in S : x \sim y\} \\ &= cl(x)\end{aligned}$$

This means Orbits of elements of the non empty set forms a class or precisely forms an equivalence class of x . So it is clear that Orbits follows all properties of an equivalence class. So, our conclusion is,

1. The Orbits of x are either disjoint or equal.
2. The set S is a disjoint union of its Orbits.
3. The Orbits can be uniquely represented geometrically.

5. References

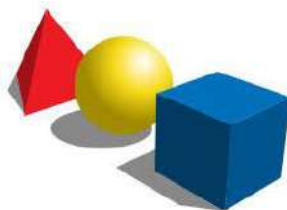
1. Wolfram Math world
2. Fundamentals of Abstract Algebra-
D.S.Malik
John N.Mordeson
M.K.Sen



PROJECT:-GROUP THEORY APPLICATION

STUDENTS PARTICIPATED:-

<u>NAME</u>	<u>ROLL</u>
I)SHOUNAK CHAKROBORTY	364
II)SAKIL AHAMED SARDER	347
III) PROTTUSH KR BISWAS	357
IV)TRIDEV MONDAL	359



SUPERVISED BY

PRAVANJAN KUMAR RANA

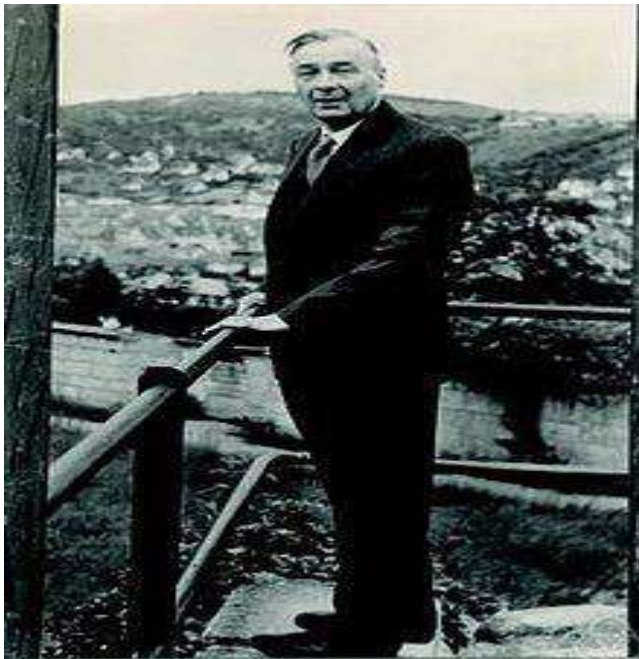
ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our respected teacher **Pravanjan Kumar Rana** who gave us the golden opportunity to do this wonderful project on **Group theory Application**. we got to learn a lot more, from this project about **hall subgroup** which will be very helpful for us.

In the end, we would like to thank our team. Without them, would not have been able to complete this project.

HALL SUBGROUP;AN APPLICATION OF SYLOW THEOREM

INTRODUCTION



Philip Hall (11 April 1904 – 30 December 1982), was an English mathematician. His major work was on group theory, notably on finite groups and solvable groups.

He was educated first at Christ's Hospital, where he won the Thompson Gold Medal for mathematics, and later at King's College Cambridge. He was elected a Fellow of the Royal Society in 1951 and awarded its Sylvester medal in 1961. He was President of the London Mathematical Society in 1955–1957, and awarded its Berwick Prize in 1958 and De Morgan Medal in 1965.

HALL SUBGROUP

In mathematics, a **Hall subgroup** of a finite group, G is a subgroup whose order is coprime to its index. They were introduced by the group theorist Phillip hall (1928).

DEFINATION

A **Hall divisor** (also called a unitary division) of an integer n is a divisor d of n such that d and n/d are coprime. The easiest way to find the Hall divisors is to write the **prime factorization** for the number in question and take any product of the multiplicative terms (the full power of any of the prime factors), including 0 of them for a product of 1 or all of them for a product equal to the original number.

For example, to find the Hall divisors of 60, show the prime factorization is $2^2 \cdot 3 \cdot 5$ and take any product of $\{3,4,5\}$. Thus, the Hall divisors of 60 are 1, 3, 4, 5, 12, 15, 20, and 60.

A **Hall subgroup** of G is a subgroup whose order is a Hall divisor of the order of G . In other words, it is a subgroup whose order is coprime to its index.

EXAMPLES

- Any Sylow subgroup of a group is a Hall subgroup.
- If $G = A_5$, the only simple group of order 60, then 15 and 20 are Hall divisors of the order of G , but G has no subgroups of these orders.
- The simple group of order 660 has two Hall subgroups of order 12 that are not even isomorphic (and so certainly not conjugate, even under an outer automorphism). The normalizer of a Sylow 2-subgroup of order 4 is isomorphic to the alternating group A_4 of order 12, while the normalizer of a subgroup of order 2 or 3 is isomorphic to the dihedral group of order 12.

HALL'S THEOREM

Hall proved that if G is a [finite solvable group](#) and π is any set of primes, then G has a [Hall \$\pi\$ -subgroup](#), and any [two Hall \$\pi\$ -subgroups](#) are conjugate.

Moreover, any subgroup whose order is a product of primes in π is contained in some [Hall \$\pi\$ -subgroup](#).

This result can be thought of as a generalization of [Sylow's Theorem](#) to [Hall subgroups](#), but the examples above show that such a generalization is false when the group is not solvable.

The existence of [Hall subgroups](#) can be proved by [induction](#) on the order of G , using the fact that every [finite solvable group](#) has a normal elementary [abelian subgroup](#).

More precisely, fix a minimal [normal subgroup](#) A , which is either a π -group or a π' -group as G is π -separable.

By [induction](#) there is a [subgroup](#) H of G containing A such that H/A is a [Hall \$\pi\$ -subgroup](#) of G/A . If A is a π -group then H is a Hall π -subgroup of G . On the other hand, if A is a π' -group, then by the [Schur-Zassenhaus theorem](#), A has a complement in H , which is a Hall π -subgroup of G .

CONVERSE TO HALL'S THEOREM

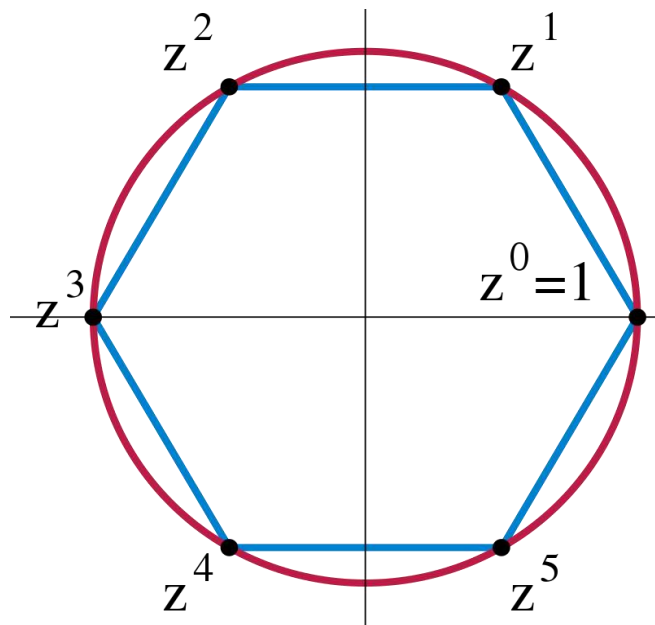
Any finite group that has a [Hall \$\pi\$ -subgroup](#) for every set of primes π is solvable. This is a generalization of [Burnside's theorem](#) that any group whose order is of the form $p^a q^b$ for primes p and q is solvable, because [Sylow's theorem](#) implies that all [Hall subgroups exist](#). This does not (at present) give another proof of Burnside's theorem, because Burnside's theorem is used to prove this [converse](#).

SYLOW SYSTEMS

A **Sylow system** is a set of Sylow p -subgroups S_p for each prime p such that $S_p S_q = S_q S_p$ for all p and q . If we have a Sylow system, then the subgroup generated by the groups S_p for p in π is a Hall π -subgroup. A more precise version of Hall's theorem says that any solvable group has a Sylow system, and any two Sylow systems are conjugate.

NORMAL HALL SUBGROUP

Any normal Hall subgroup H of a finite group G possesses a complement, that is, there is some subgroup K of G that intersects H trivially and such that $HK = G$ (so G is a semidirect product of H and K). This is the Schur–Zassenhaus theorem.



REFERENCES

Gorenstein, Daniel (1980), *Finite groups*, New York: Chelsea Publishing Co.

Hall, Philip (1928), "**A note on soluble groups**", **Journal of the London Mathematical Society**

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE



PROJECT WORK

Topic :- Applications of Group Theory

MATHEMATICS DEPARTMENT

Submitted for partial fulfillment of the B.Sc. Degree in Mathematics

By **Suman Prasad Goswami**

COLLEGE ROLL :- **319**

REGISTRATION NO :- **A01-1112-113-011-2019**

EXAMINATION ROLL:- **2022151100**

PAPER CODE :- **MTMA CC-XII**

SEMESTER :- **5 TH (UG)**

Supervised By :- Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENTS

I gratefully acknowledge our respected Principal Maharaja for giving us inspiration and motivation.

I am grateful to my advisor **DR. PRAVANJAN KUMAR RANA** Associate Professor, Department of Mathematics, Ramakrishna Mission Vivekananda Centenary College , Kolkata-700118 for his guidance on the related area of this project work and continuous support.

I am also very much thankful to our respected teachers , whose valuable teaching and research ideas have continuously motivated me. I am also thankful to all other respected staffmembers of our department.

Finally, my deepest admiration goes to my parents for their all-out support through out my life.

Suman Prasad Goswami

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata-700118

Date:- 24/01/2022

Place:- Rahara

APPLICATION'S OF GROUP THEORY

1) ABSTRACT:-

Group Theory is one of the most important part of our daily life. Here we are going to introduce an idea how the group theory help us in TIC-TAC-TOE Game, Symmetry & Barcode.

2)INTRODUCTION:-

To fully understand the math behind group theory one needs to take a look at the theory portion of the Group Theory topic or refer to one of the reference text listed at the bottom of this project. Never the less as Chemist the object the question we are examining is usually a molecule. Though we live in the 22nd century and much is known about the physical aspects that give rise to molecular and atomic properties. The number of high level calculations that need to be performed can be both time consuming and tedious. To most experimentalist this task is takes away time and is usually not the integral part of our work. When one thinks of group theory applications one doesn't necessarily associated it with everyday life or a simple toy like a Rubik's cube.

3) MY IDEA'S:-

● Maths Problem : Tic-Tac-Toe Game (Burnside's Lemma)::

If we want to know how many different ways are there to completely fill a noughts and cross grid, using four noughts and five crosses (Not including rotations and reflections of the board)---

×	×	0
0	0	×
×	0	×

Now the answer will be 23 i.e, there are 23 different ways to completely fill a noughts and crosses grid. There are a couple ways to solve this. But we can also solve it by Mathematician's ways i.e, **BURNSIDE'S LEMMA** .

We can also solve it by using rotations and reflections, but that will be very lengthy.



First of all, how can we fill 3×3 grids, using four noughts and five crosses = $\frac{9!}{4! \times 5!}$

$$=126$$

0 0 0 0

× × × × ×

We can use Burnside's Lemma to determine the required number .

Here we consider Eight Symmetries – Identity ,90° rotation, 180° rotation, 270° rotation and four reflection.

Burnside Lemma ::

$$\text{Total number of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

[the number of orbits is equal to the average number of fixed points.]

We can substitute the size of the group $|G|=8$

First we consider the fixed elements of the identity.

For identity, there are 126 grids that remains unchanged. So its fix size=126.

Now we consider the fix size for the 90° rotation. For 90° rotation there are only two grids that remain unchanged . So its fix size=2.

Simmilarlly, 180° and 270° rotation the fix size are 6 and 2 respectively.

For a rotation, either side of the reflection will have to look the same. Here we find 12 grids that remain unchanged.

So for each reflection the fix size=12

Total fixed size=126+2+6+2+12+12+12+12

=184.

By Burnside's Lemma number of orbits = $\frac{184}{8}$

= 23.

● Symmetry (In Chemistry)::

The dihedral group can be defined as the group of symmetries n-gon ,and such a geometric definition is easier to graso because it is very visual as opposed to an abstract definition. We learned that the dihedral group (D_n) was defined as

$$D_n = \{e, r^k, s, r^k s\} \text{ (k and n both integers) where}$$

- 1) The identity operation (e) causes no change.
- 2) The rotation operation r^k (also called proper rotation) where $k=\{1,n\}$ is a counterclockwise rotation of $k \frac{360^\circ}{n}$ about a rotation axis. Where $k=n$, $r^n = e$ (Since rotation of 360° is the identity operation

- 3) The reflection operation (σ) exchanges left & right, as if each point had moved perpendicularly through the plane to a position exactly as far from the plane as it started. If k is even, $k=2p$, $\sigma^{2p}=e$
- 4) A rotation-reflection operation (σ^k) (Sometimes called an improper rotation) requires a rotation of k ($360^\circ/n$) followed by reflection through a plane perpendicular to the axis of rotation.

In this section, we decided to look primarily at symmetry operations of simple linear molecules from geometric and group theoretical approach. I choose a basic linear molecule carbon dioxide (CO_2) which has the following molecule representations:

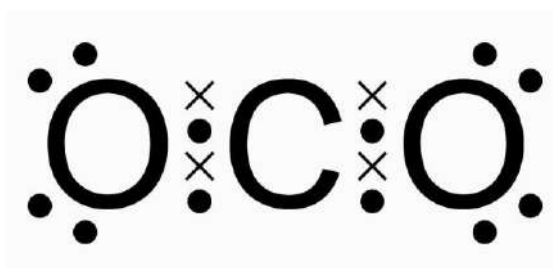


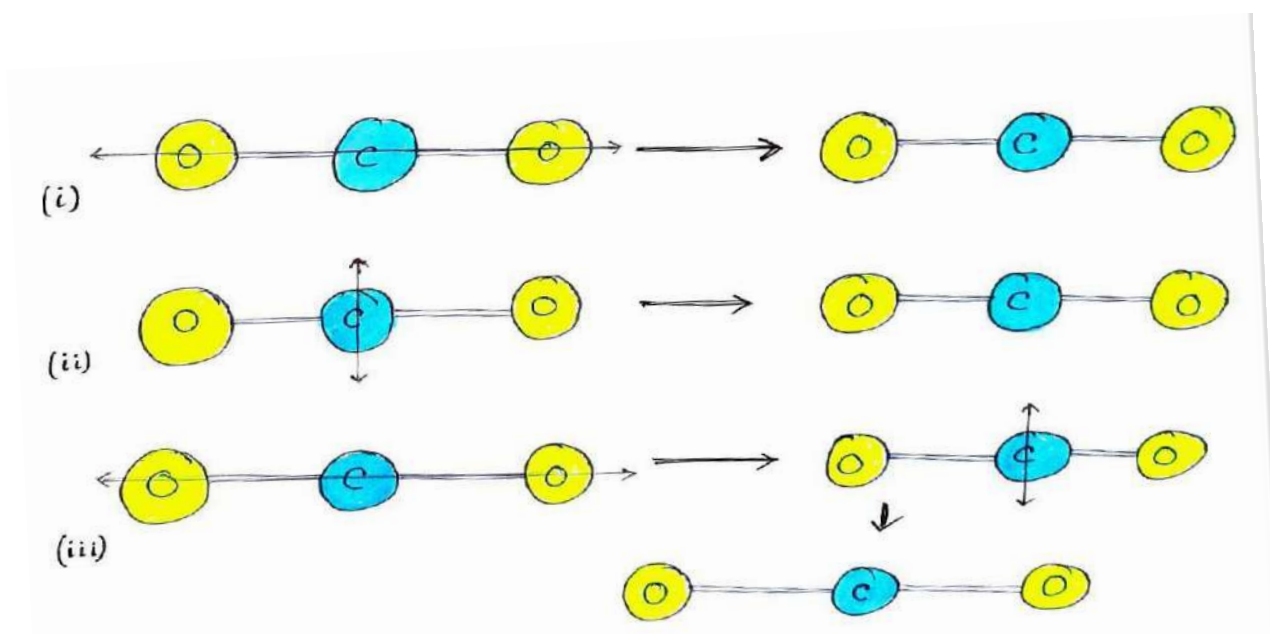
Figure-1



Figure-2

Observing figure-1 the Lewis structure of CO_2 . Oxygen atom has six valence electrons and carbon has four valence electrons and CO_2 is sp hybridized. So CO_2 is linear and planar structure. In this case to maximize distance, the atoms form a 180° angle with the centralized atom as a vertex. Looking at Figure-2 it is very easy to see the symmetry operations for CO_2 .

- (1) A rotation around a central horizontal C_∞ axis
- (2) A reflection about a central and then
- (3) a composition of 1 & 2 or a rotation followed by a reflection. The identity operation (e) is also a symmetry operation.



Now, if we see in the structure Boron Trifluoride (BF_3) then 24 valence electrons are there and its an SP^2 hybridization. So, its Triangle planner i.e, it's same as D_3 . So we can apply rotation & reflection

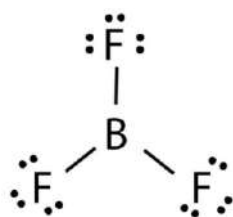


Figure :- BF_3

And when we see in the structure Xenon Tetrafluoride and it's (XeF_4), has 36 valence electrons and SP^3d^2 hybridization and it's square planner structure. i.e, it's same as D_4 i.e, we can take the operation rotation 90° , rotation 180° , rotation 270° , reflection horizontally, reflection vertically, reflection in main main diagonally and reflection with respect to another diagonal.

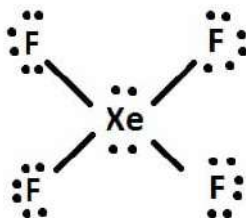


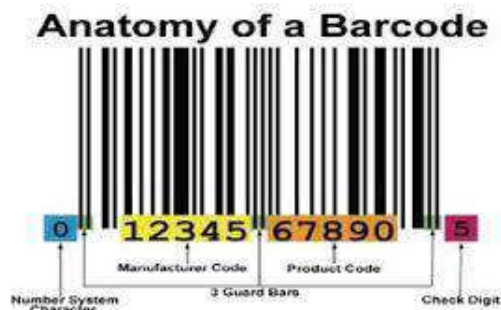
Figure :- XeF_4

● Barcode::

We also know as Universal Product Code (UPC). A UPC-A identification number has 12- digits. The first six digits identify manufacture, the next five digits identify the product and 1st is a check An item with UPC identification number

$$(a_1, a_2, \dots, a_{12})(3, 1, 3, 1, \dots, 3, 1) \bmod 10 = 0.$$

Now suppose a single error is made in entering the the number in computer , it won't satisfy the condition.



::Conclusion::

In this project, we want to discuss some applications of group theory. We know the theory portion, but if don't know the application of that then it's like 'I have a car, but I don't know the drive'. So when we read dihedral group then from that portion we want to discuss symmetrical structure of some chemical compounds, i.e, from here we can conclude that in chemistry we can see application of group theory. After that when we want to solve in how many ways are there obviously in different ways to complete the Tic-Tac-Toe game by four noughts and five crosses, then we can solve it by rotation and reflection of the board and Interchanging of grids. Then we get the answer 23 .But it's very lengthy process, but if we solve it by group action mainly by Burnside Lemma, we can easily solve this. So from here we can conclude that in game there are application of group theory.

::Reference::

- 1) Contemporary Abstract Algebra; Joseph A. Gallian
- 2) Fundamental of Abstract Algebra; D.S.Malik,, John N. Mordeson,, M.K.Sen.
- 3) Chemistry (Inorganic & Organic); Dr.Rabindranath Maiti, Nemai Tewari, Sabithabrata Roy.

RKMVCC RAHARA

Department of Mathematics

Semester: 5th

Core Course-XII

Group Theory-II

Project member:

Koushik Chatterjee

Exam Roll-2022151104

Reg No.-A01-1112-113-015-2019

Supervised by:

Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and my special gratitude to **Dr. Prabanjan kumar Rana, head of the department mathematics of RKMVCC Rahara**, who gave me a golden opportunity to do this project and also provided support in completing my project work.

I would also like to extend my gratitude to my friend Ritoprovo Roy, who helped me by sketching the drawings for my project.

TOPIC

Geometry of Orbits in Three Dimensional Sphere

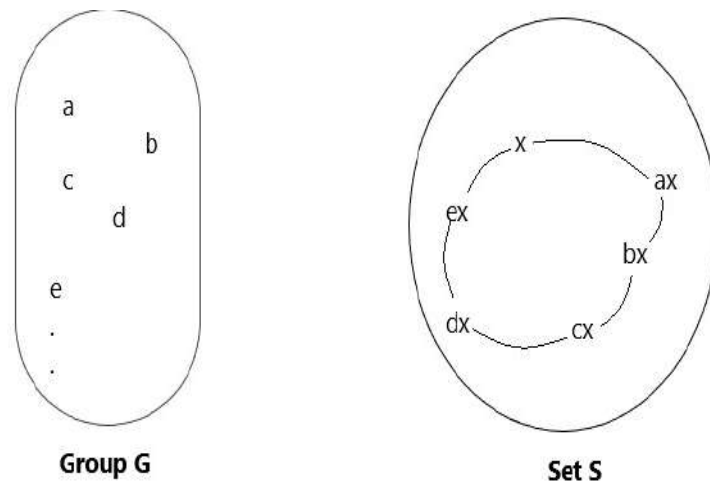
1. Abstract:

In this context we discussed geometry of orbits in light of three dimensional systems especially in a Sphere. Here we consider the group G as $(\mathbb{R}, +)$ and the set S as \mathbb{R}^2 . When S is a G set, we denote the group action by $\varphi: G \times S \rightarrow S$. Here the orbits orient themselves as a plane in three dimensional geometry containing three axes "X", "Y" & "Z" .

2. Introduction:

Let, G be any group whose elements are of the form $\{a, b, c, d, \dots e\}$. Also let S be a nonempty set & $x \in S$.

Keeping the element x fixed, we take all the elements of the form gx where $g \in G$ from the set S .



The set that contains elements of the form gx where $g \in G$, where x is a fixed element, is called the Orbit of x .

2.1 Definition of orbit:

Let, G be a group, acting on a non-empty set S . If $x \in S$, then the trajectory $\{\varphi(g, x): g \in G\}$ of the point x is called the orbit of the point x . It is denoted by O_x or by $[x]$.

2.2. Definition respect to equivalence relation:

Let, G be a group, acting on a non-empty set S . Now we define a relation ' \sim ' on S by $a \sim b \Leftrightarrow ga = b$ for some $g \in G$ & $\forall a, b \in S$. Then the relation ' \sim ' is an equivalence relation.

- The equivalence classes determined by the equivalence relation ' \sim ' are called the Orbits of G on S .

3. Concept of geometry of orbits:

For ease of understanding we can imagine the universe as a group. Then we can observe that every planet has own Orbit. We have the orbits never intersects with each other and they follow their own path. Each and every orbit has their different pattern of different shapes. We will discuss this in this context.

EXAMPLE-3.1: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x + t, y) \forall t \in G \ (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

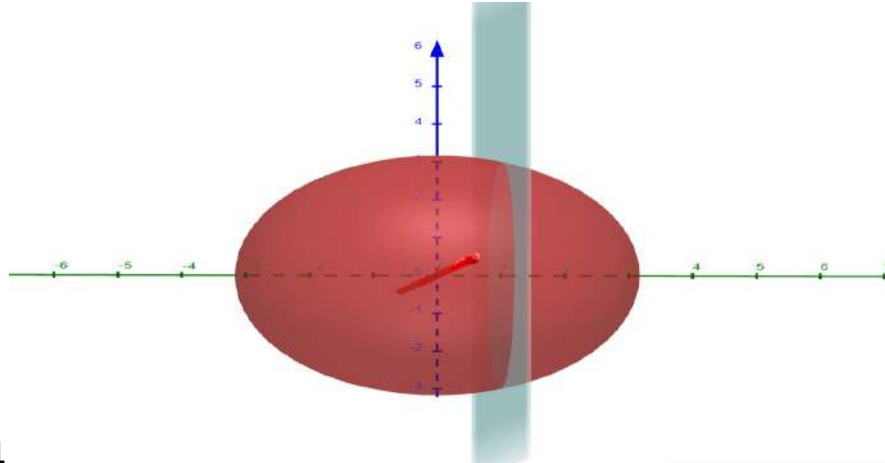
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), 1: t \in \mathbb{R}\}$$

$$\{(x, 1): x \in \mathbb{R}\}; \text{ where } (1 + t) = x$$

For this case the Y coordinate is always 1

i.e. horizontal line parallel to X axis, above the origin



Picture-1

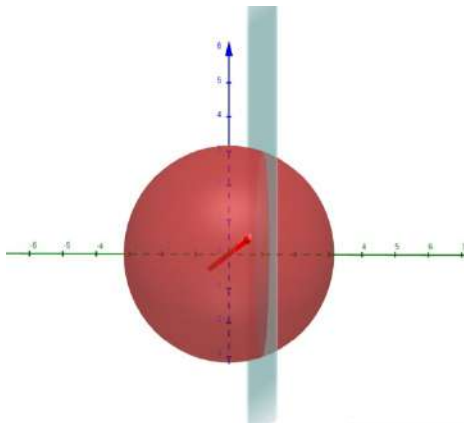
Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), b: t \in \mathbb{R}\}$
 $\{(x, b): x \in \mathbb{R}\};$ where $(a + t) = x$

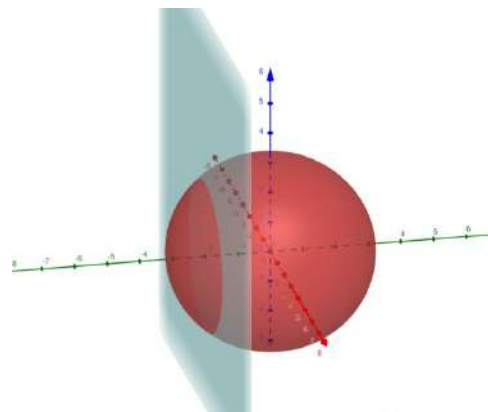
For this case Y coordinate is always b

When $b > 0$, the line is above origin, parallel to X axis

When $b < 0$, the line is below origin, parallel to X axis.



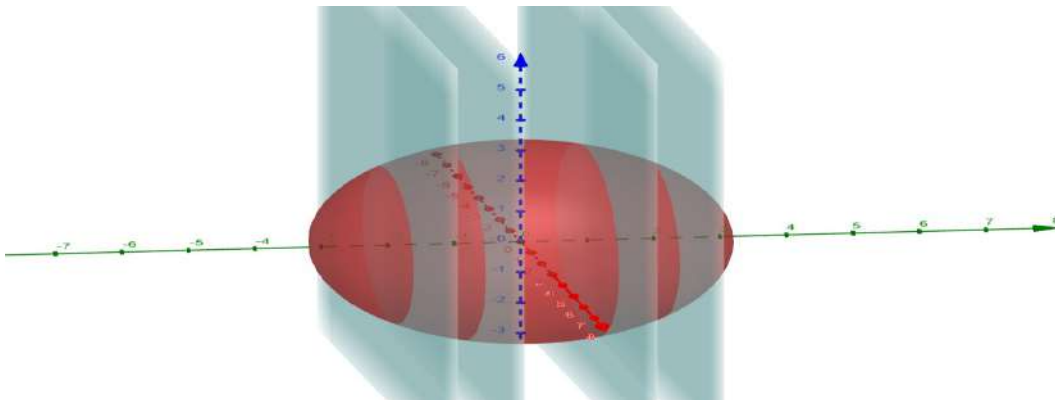
Picture-2



Picture-3

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-4

Blue line= X axis

Green line= Y axis

Red line= Z axis

EXAMPLE-3.2: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x, y + t) \forall t \in G \text{ and } (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

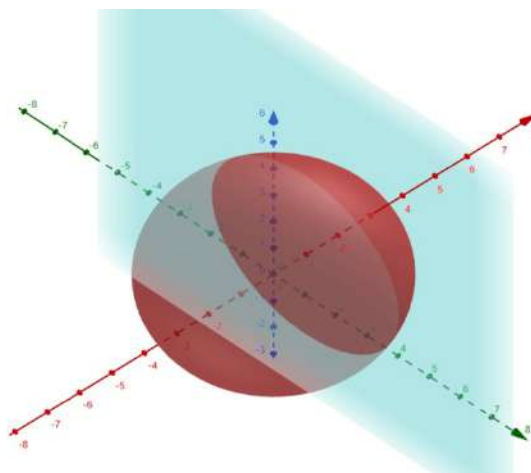
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{1, (1 + t): t \in \mathbb{R}\}$$

$$\{(1, y): x \in \mathbb{R}\}; \text{ where } (1 + t) = y$$

For this case the X coordinate is always 1

i.e. horizontal line parallel to Y axis.



Picture-5

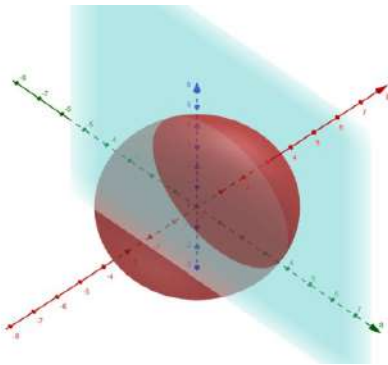
Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{a, (t + b): t \in \mathbb{R}\}$
 $\{(a, y): x \in \mathbb{R}\}$; where $(b + t) = y$

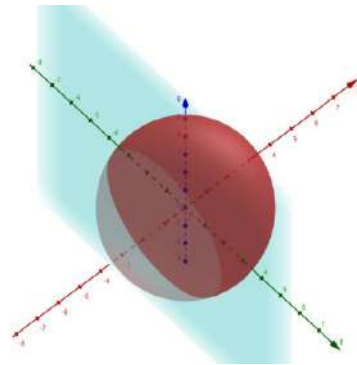
For this case X coordinate is always a

When $a > 0$, the line lies on right side of the origin, parallel to Y axis

When $a < 0$, the line lies on left side of the origin, parallel to Y axis.



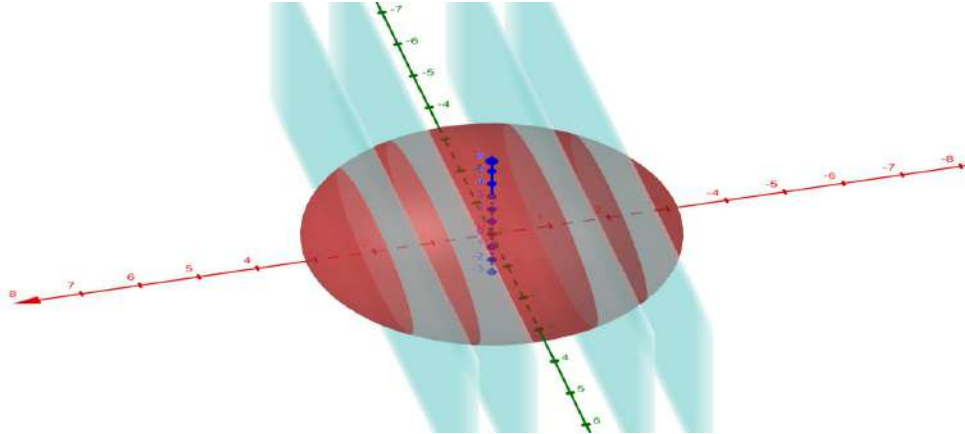
Picture-6



Picture-7

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-8

Blue line= X axis
Green line= Y axis
Red line= Z axis

EXAMPLE-3.3: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map $\alpha: G * S \rightarrow S$ by $\alpha\{t, (x, y)\} = t. (x, y) := (x + t, y + t) \forall t \in G \text{ and } (x, y) \in \mathbb{R}^2$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

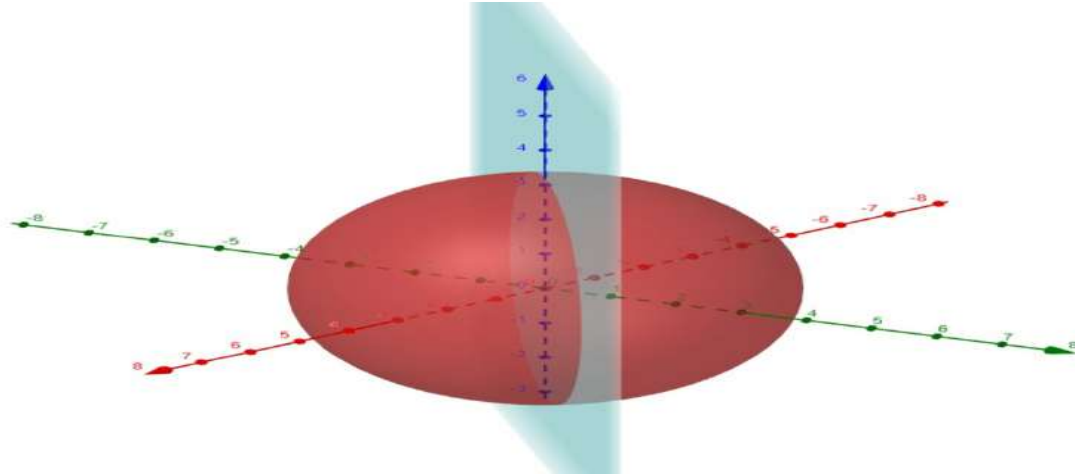
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), (1 + t): t \in \mathbb{R}\}$$

$$\{(x, x): x \in \mathbb{R}\} ; \text{ where } (1 + t) = x$$

As x is a arbitrary real number and $y = x$ so it passes through the origin and slope 1.

The picture is given below,



Picture-9

Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), (t + b): t \in \mathbb{R}\}$

As $t \in \mathbb{R}$ so take two different values of t namely $t = 0$ and $t = 1$

Then we have the required line passes through the points (a, b) & $(a + 1, b + 1)$

Equation of the line will be: $\frac{y - y_2}{y_1 - y_2} = \frac{x - x_2}{x_1 - x_2}$

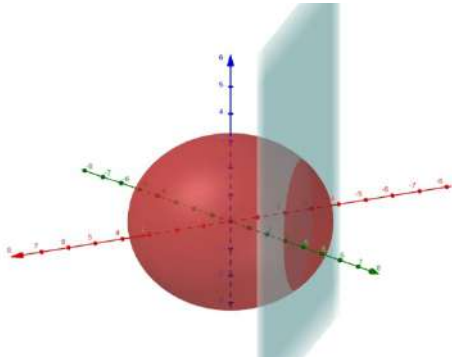
$$\text{Or, } \frac{y - b}{b + 1 - b} = \frac{x - a}{a + 1 - a}$$

$$\text{Or, } x - y = (a - b)$$

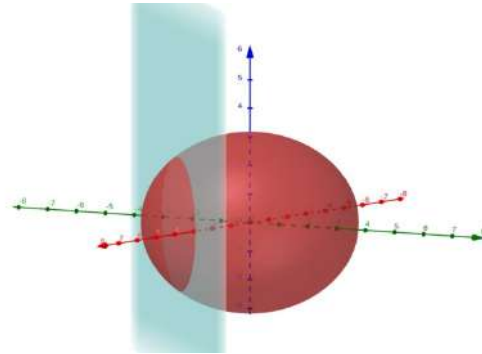
$$\text{Or, } y = x - (a - b)$$

This shows that the slope is 1 but the intercept is non zero.

When $a > b$, the intercept is negative and When $a < b$, the intercept is positive.



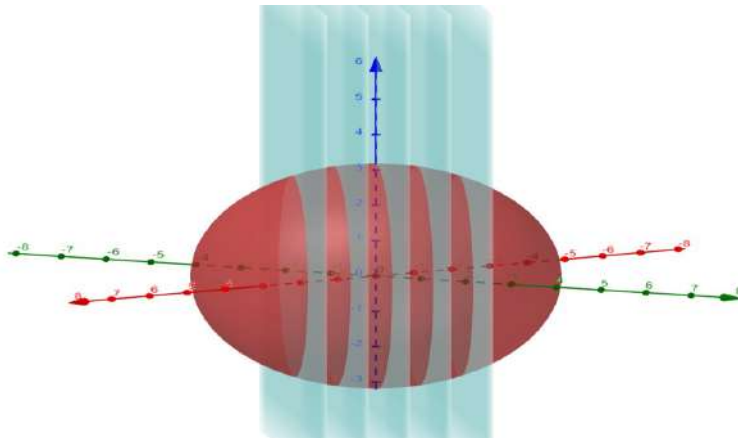
Picture-10



Picture-11

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-12

Blue line= X axis
Green line= Y axis
Red line= Z axis

4. Conclusion

Let G be a group and S be a non empty set. Suppose $x \in S$. Then, we wish to find the notation for Orbit of x .

Orbit of x , denoted by

$$\begin{aligned}[x] &= \{g \cdot x : g \in G\} \\ &= \{y \in S : y = g \cdot x \text{ for some } g \in G\} \\ &= \{y \in S : x \sim y\} \\ &= cl(x)\end{aligned}$$

This means Orbits of elements of the non empty set forms a class or precisely forms an equivalence class of x . So it is clear that Orbits follows all properties of an equivalence class. So, our conclusion is,

1. The Orbits of x are either disjoint or equal.
2. The set S is a disjoint union of its Orbits.
3. The Orbits can be uniquely represented geometrically.

5. References

1. Wolfram Math world
2. Fundamentals of Abstract Algebra-
D.S.Malik
John N.Mordeson
M.K.Sen



RKMVCC, Rahara
Department of Mathematics

GROUP THEORY

Geometric Representation Group Action

Nayan Kumar Chakraborty

Supervisor: **Dr. Pravanjan Kumar Rana**

January 12, 2022

Rahara

Contents

1	Acknowledgments	3
2	Dedication	4
3	Introduction	5
4	The main content	6
4.1	Definitions	6
4.2	Visual Representation of Group Actions	7
4.2.1	The group action $\phi(g, x) = g.x$	7
4.2.2	The trivial group action	7
4.3	On any generalised geometric set X and any group G	8
5	Conclusions	9

Acknowledgments

I would express my gratitude and thanks to Dr. Pravanjan Kumar Rana, Head of Department Mathematics, Ramakrishna Mission Vivekananda Centenary College Rahara for providing me the opportunity to work on this innovative project. I would also like to thank my group Ritoprovo Roy and Supriyo Pal who co-operated me in completing my project. I would like to thank my parents who provided me moral support and kept patience with me.

Dedication

I dedicate this project in the spirit of Swami Vivekananda and his moral principles which moved me greatly and helped me in every course of my life.

Introduction

This project work is an extension of Shailesh Shirali's work on the topic "Groups Associated with Conics" where he focused on how Abelian Groups can be visualised using conic sections. In this project investigation we have tried to visualise Group Actions on Sets by Abelian Groups using three dimensional spatial co-ordinates. In this paper we work on the field \mathbb{R} of real numbers in general. We have tried to visualise group actions of Abelian groups in general over some particular sets. On geometric interpretation, we see interesting patterns and figures emerge out of them. Later we give an attempt to generalise this notion over any sets. We also attempt to show a geometric visualisation of Cayley's Theorem using Group Actions.

All figures and plotting made necessary in this project are designed entirely using python language.

The main content

We consider a non-degenerate conic Γ and consider any fixed point in the conic. Let the point be called 'N'. This point will be our identity element throughout our discussion. We consider the space \mathbb{R}^3 for our project.

4.1 Definitions

We define the following important terms:

1. Group : A group is a set S with a binary operation $\oplus : S \times S \rightarrow S$ such that it satisfies the following properties :

i)Associative : For any $a, b, c \in S$ we must have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

ii)Inverse : For every element $a \in S$, $\exists b \in S$ such that $a \oplus b = e$.

iii)Identity : $\exists e \in S$ such that $a \oplus e = e \oplus a = a, \forall a \in S$.

2. Abelian Group : A group in which the binary operation is commutative.

3. Group Action : A group G is set to be acting on a set X when there is a map $\phi : G \times X \rightarrow X$, such that the following conditions hold for all elements $x \in X$.

i) $\phi(e, x) = x$

ii) $\phi(g, \phi(h, x)) = \phi(g \oplus h, x), \forall g, h \in G$.

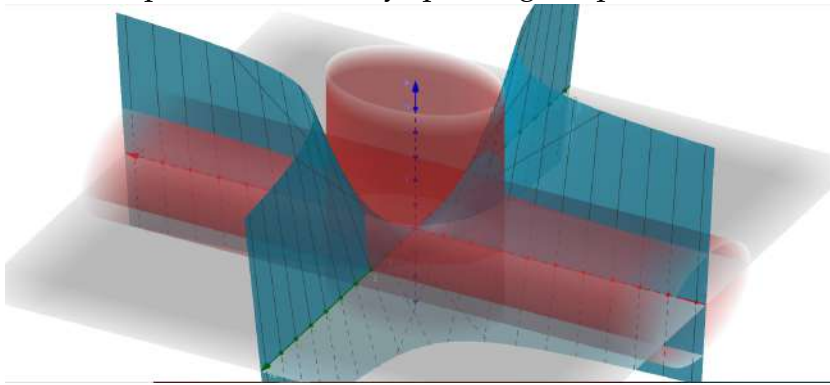
The rest of the definitions for this project are used from [1].

4.2 Visual Representation of Group Actions

We consider an Abelian group G and represent it by a non-degenerate conic in three dimensional space. We do some case studies of some particular examples of group actions.

4.2.1 The group action $\phi(g, x) = g.x$

We try to visualise the group action G on itself by left multiplication action. Hence we try to project the conic representation of G on the points of the graph $f(x, y) = x * y$. Since we are working with Abelian groups on the field \mathbb{R} our left multiplication so called corresponds to normal multiplication. Visually speaking the plot looks like this:

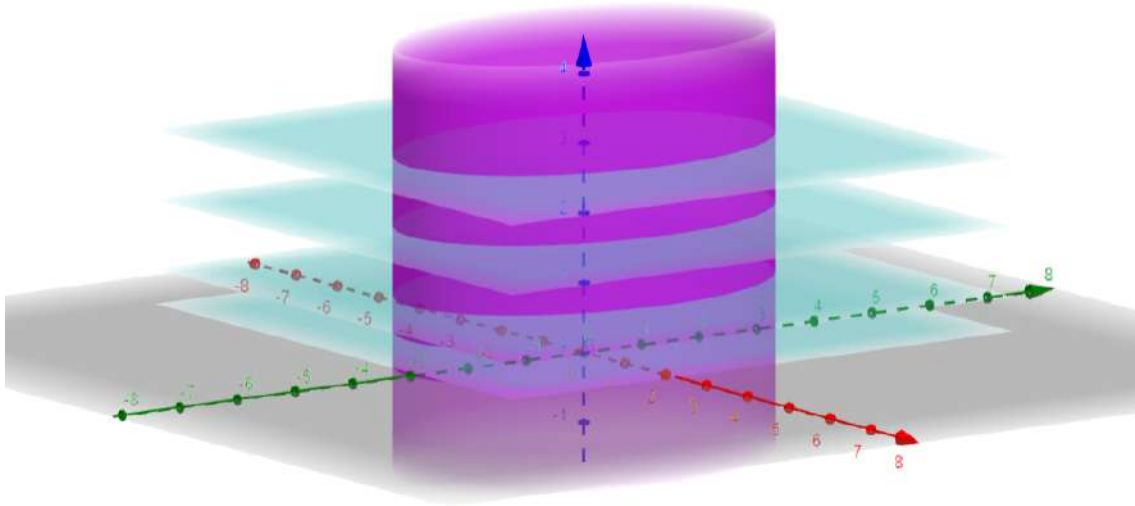


The group action here is the intersection of the 3 plots region as shown in the figure.

4.2.2 The trivial group action

We try to visualise the trivial group action of a group G on the set X . Then the trivial group action is given by $\phi(g, x) = x, \forall x \in X$. In this group action every element of g induces the identity permutation on X .

Visually speaking the plot for this group action takes the shape of X . For example if we consider the group G and any discrete set X the group action diagram looks like the figure below:



From this above diagram we realise that the group action on X is basically the projection of the Abelian group G on the set X . The conic here is the Abelian group G .

4.3 On any generalised geometric set X and any group G

We are now in a position to resolve the situation for any set X being acted upon by an Abelian group G based upon our observations from plotting. We define a plot of a group action for an Abelian Group G on any set X by :

"Projection of the plot of G over the plot of the set X following the rule for ϕ ".

For non-Abelian groups, we can implement the same method to visualise Group actions for any set X on which they are acting upon. These visualisations help us understand the nature of the group actions.

Conclusions

From our observations and formulations we see that that a group action ϕ of G defined on a set X can graphically be visualised as a projection of G over the set X following ϕ . Such visualisations are made possible currently for Abelian groups because of the work of Shailesh Shirali on his paper [1]. Group actions are useful in various fields of chemistry, biology and related fields. The author of this paper is convinced that visualising group actions is essential for solving many real life problems faced currently in applied fields.

Bibliography

- [1] Shailesh Shirali, Groups Associated with Conics. *Mathematical Gazette*, 2009.
- [2] Keith Conrad. Group Theory. <https://kconrad.math.uconn.edu/blurbs/>
- [3] Dummit Foote , <https://www.wiley.com/en-us/Abstract+Algebra>



RKMVCC, Rahara
Department of Mathematics

GROUP THEORY

Geometric Representation Group Action

Supriyo Pal

Supervisor: **Dr. Pravanjan Kumar Rana**

January 12, 2022

Rahara

Contents

1	Acknowledgments	3
2	Dedication	4
3	Introduction	5
4	The main content	6
4.1	Definitions	6
4.2	Visual Representation of Group Actions	7
4.2.1	The group action $\phi(g, x) = g.x$	7
4.2.2	The trivial group action	7
4.3	On any generalised geometric set X and any group G	8
5	Conclusions	9

Acknowledgments

I would express my gratitude and thanks to Dr. Pravanjan Kumar Rana, Head of Department Mathematics, Ramakrishna Mission Vivekananda Centenary College Rahara for providing me the opportunity to work on this innovative project. I would also like to thank my group Ritoprovo Roy and Nayan Kumar Chakraborty who co-operated me in completing my project. I would like to thank my parents who provided me moral support and kept patience with me.

Dedication

I dedicate this project in the spirit of Swami Vivekananda and his moral principles which moved me greatly and helped me in every course of my life.

Introduction

This project work is an extension of Shailesh Shirali's work on the topic "Groups Associated with Conics" where he focused on how Abelian Groups can be visualised using conic sections. In this project investigation we have tried to visualise Group Actions on Sets by Abelian Groups using three dimensional spatial co-ordinates. In this paper we work on the field \mathbb{R} of real numbers in general. We have tried to visualise group actions of Abelian groups in general over some particular sets. On geometric interpretation, we see interesting patterns and figures emerge out of them. Later we give an attempt to generalise this notion over any sets. We also attempt to show a geometric visualisation of Cayley's Theorem using Group Actions.

All figures and plotting made necessary in this project are designed entirely using python language.

The main content

We consider a non-degenerate conic Γ and consider any fixed point in the conic. Let the point be called 'N'. This point will be our identity element throughout our discussion. We consider the space \mathbb{R}^3 for our project.

4.1 Definitions

We define the following important terms:

1. Group : A group is a set S with a binary operation $\oplus : S \times S \rightarrow S$ such that it satisfies the following properties :

i)Associative : For any $a, b, c \in S$ we must have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

ii)Inverse : For every element $a \in S$, $\exists b \in S$ such that $a \oplus b = e$.

iii)Identity : $\exists e \in S$ such that $a \oplus e = e \oplus a = a, \forall a \in S$.

2. Abelian Group : A group in which the binary operation is commutative.

3. Group Action : A group G is set to be acting on a set X when there is a map $\phi : G \times X \rightarrow X$, such that the following conditions hold for all elements $x \in X$.

i) $\phi(e, x) = x$

ii) $\phi(g, \phi(h, x)) = \phi(g \oplus h, x), \forall g, h \in G$.

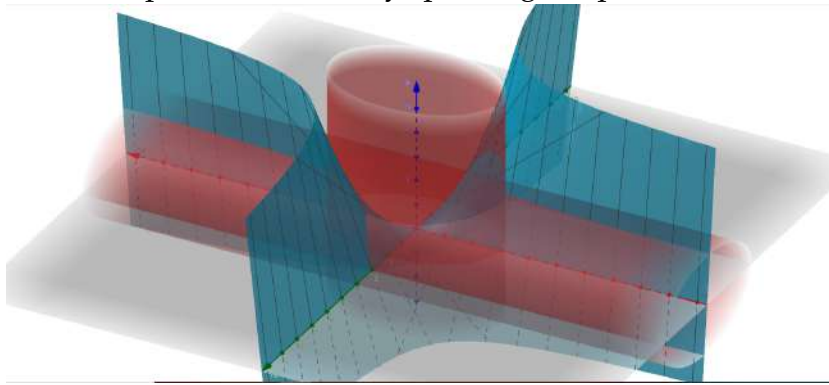
The rest of the definitions for this project are used from [1].

4.2 Visual Representation of Group Actions

We consider an Abelian group G and represent it by a non-degenerate conic in three dimensional space. We do some case studies of some particular examples of group actions.

4.2.1 The group action $\phi(g, x) = g.x$

We try to visualise the group action G on itself by left multiplication action. Hence we try to project the conic representation of G on the points of the graph $f(x, y) = x * y$. Since we are working with Abelian groups on the field \mathbb{R} our left multiplication so called corresponds to normal multiplication. Visually speaking the plot looks like this:

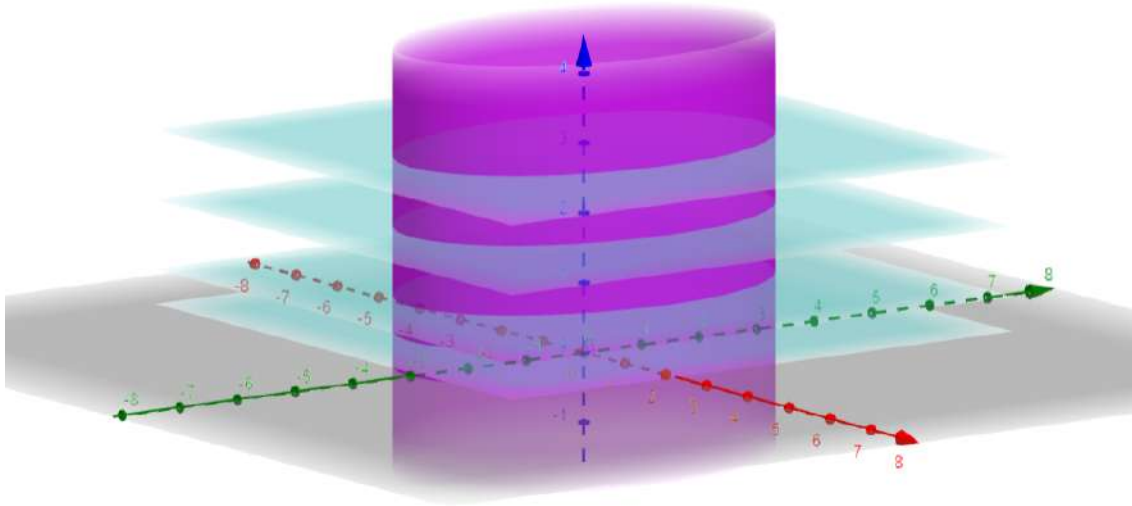


The group action here is the intersection of the 3 plots region as shown in the figure.

4.2.2 The trivial group action

We try to visualise the trivial group action of a group G on the set X . Then the trivial group action is given by $\phi(g, x) = x, \forall x \in X$. In this group action every element of g induces the identity permutation on X .

Visually speaking the plot for this group action takes the shape of X . For example if we consider the group G and any discrete set X the group action diagram looks like the figure below:



From this above diagram we realise that the group action on X is basically the projection of the Abelian group G on the set X. The conic here is the Abelian group G.

4.3 On any generalised geometric set X and any group G

We are now in a position to resolve the situation for any set X being acted upon by an Abelian group G based upon our observations from plotting. We define a plot of a group action for an Abelian Group G on any set X by :

"Projection of the plot of G over the plot of the set X following the rule for ϕ ".

For non-Abelian groups, we can implement the same method to visualise Group actions for any set X on which they are acting upon. These visualisations help us understand the nature of the group actions.

Conclusions

From our observations and formulations we see that that a group action ϕ of G defined on a set X can graphically be visualised as a projection of G over the set X following ϕ . Such visualisations are made possible currently for Abelian groups because of the work of Shailesh Shirali on his paper [1]. Group actions are useful in various fields of chemistry, biology and related fields. The author of this paper is convinced that visualising group actions is essential for solving many real life problems faced currently in applied fields.

Bibliography

- [1] Shailesh Shirali, Groups Associated with Conics. *Mathematical Gazette*, 2009.
- [2] Keith Conrad. Group Theory. <https://kconrad.math.uconn.edu/blurbs/>
- [3] Dummit Foote , <https://www.wiley.com/en-us/Abstract+Algebra>



RKMVCC, Rahara
Department of Mathematics

GROUP THEORY

Geometric Representation Group Action

Ritoprovo Roy

Supervisor: **Dr. Pravanjan Kumar Rana**

January 12, 2022

Rahara

Contents

1	Acknowledgments	3
2	Dedication	4
3	Introduction	5
4	The main content	6
4.1	Definitions	6
4.2	Visual Representation of Group Actions	7
4.2.1	The group action $\phi(g, x) = g.x$	7
4.2.2	The trivial group action	7
4.3	On any generalised geometric set X and any group G	8
5	Conclusions	9

Acknowledgments

I would express my gratitude and thanks to Dr. Pravanjan Kumar Rana, Head of Department Mathematics, Ramakrishna Mission Vivekananda Centenary College Rahara for providing me the opportunity to work on this innovative project. I would also like to thank my group Nayan Kumar Chakraborty and Supriyo Pal who co-operated me in completing my project. I would like to thank my parents who provided me moral support and kept patience with me.

Dedication

I dedicate this project in the spirit of Swami Vivekananda and his moral principles which moved me greatly and helped me in every course of my life.

Introduction

This project work is an extension of Shailesh Shirali's work on the topic "Groups Associated with Conics" where he focused on how Abelian Groups can be visualised using conic sections. In this project investigation we have tried to visualise Group Actions on Sets by Abelian Groups using three dimensional spatial co-ordinates. In this paper we work on the field \mathbb{R} of real numbers in general. We have tried to visualise group actions of Abelian groups in general over some particular sets. On geometric interpretation, we see interesting patterns and figures emerge out of them. Later we give an attempt to generalise this notion over any sets. We also attempt to show a geometric visualisation of Cayley's Theorem using Group Actions.

All figures and plotting made necessary in this project are designed entirely using python language.

The main content

We consider a non-degenerate conic Γ and consider any fixed point in the conic. Let the point be called 'N'. This point will be our identity element throughout our discussion. We consider the space \mathbb{R}^3 for our project.

4.1 Definitions

We define the following important terms:

1. Group : A group is a set S with a binary operation $\oplus : S \times S \rightarrow S$ such that it satisfies the following properties :

i)Associative : For any $a, b, c \in S$ we must have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

ii)Inverse : For every element $a \in S$, $\exists b \in S$ such that $a \oplus b = e$.

iii)Identity : $\exists e \in S$ such that $a \oplus e = e \oplus a = a, \forall a \in S$.

2. Abelian Group : A group in which the binary operation is commutative.

3. Group Action : A group G is set to be acting on a set X when there is a map $\phi : G \times X \rightarrow X$, such that the following conditions hold for all elements $x \in X$.

i) $\phi(e, x) = x$

ii) $\phi(g, \phi(h, x)) = \phi(g \oplus h, x), \forall g, h \in G$.

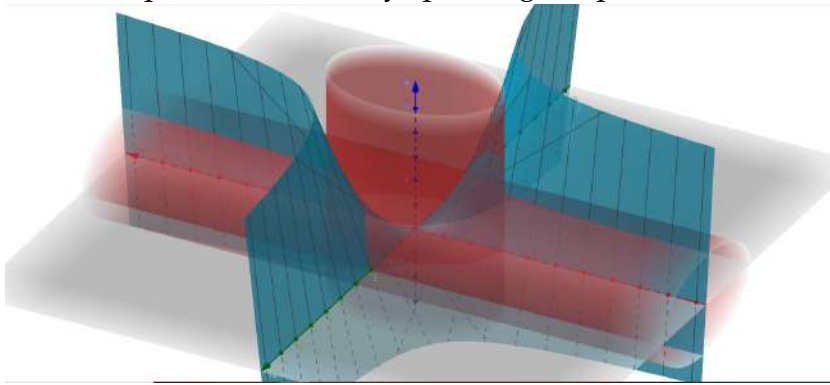
The rest of the definitions for this project are used from [1].

4.2 Visual Representation of Group Actions

We consider an Abelian group G and represent it by a non-degenerate conic in three dimensional space. We do some case studies of some particular examples of group actions.

4.2.1 The group action $\phi(g, x) = g.x$

We try to visualise the group action G on itself by left multiplication action. Hence we try to project the conic representation of G on the points of the graph $f(x, y) = x * y$. Since we are working with Abelian groups on the field \mathbb{R} our left multiplication so called corresponds to normal multiplication. Visually speaking the plot looks like this:

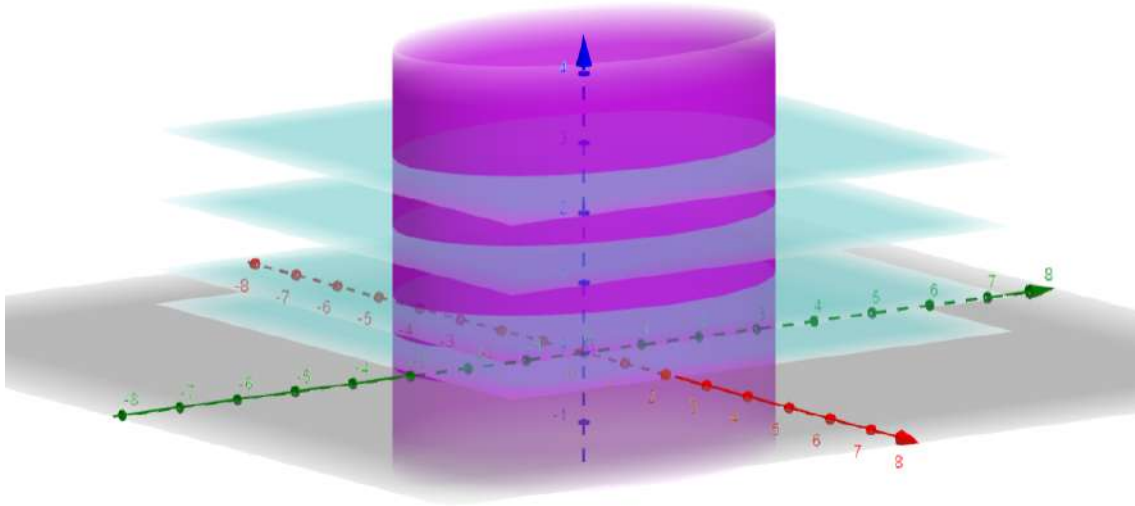


The group action here is the intersection of the 3 plots region as shown in the figure.

4.2.2 The trivial group action

We try to visualise the trivial group action of a group G on the set X . Then the trivial group action is given by $\phi(g, x) = x, \forall x \in X$. In this group action every element of g induces the identity permutation on X .

Visually speaking the plot for this group action takes the shape of X . For example if we consider the group G and any discrete set X the group action diagram looks like the figure below:



From this above diagram we realise that the group action on X is basically the projection of the Abelian group G on the set X . The conic here is the Abelian group G .

4.3 On any generalised geometric set X and any group G

We are now in a position to resolve the situation for any set X being acted upon by an Abelian group G based upon our observations from plotting. We define a plot of a group action for an Abelian Group G on any set X by :

"Projection of the plot of G over the plot of the set X following the rule for ϕ ".

For non-Abelian groups, we can implement the same method to visualise Group actions for any set X on which they are acting upon. These visualisations help us understand the nature of the group actions.

Conclusions

From our observations and formulations we see that that a group action ϕ of G defined on a set X can graphically be visualised as a projection of G over the set X following ϕ . Such visualisations are made possible currently for Abelian groups because of the work of Shailesh Shirali on his paper [1]. Group actions are useful in various fields of chemistry, biology and related fields. The author of this paper is convinced that visualising group actions is essential for solving many real life problems faced currently in applied fields.

Bibliography

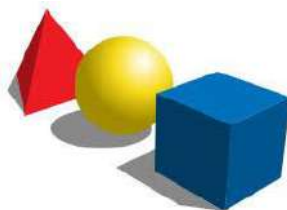
- [1] Shailesh Shirali, Groups Associated with Conics. *Mathematical Gazette*, 2009.
- [2] Keith Conrad. Group Theory. <https://kconrad.math.uconn.edu/blurbs/>
- [3] Dummit Foote , <https://www.wiley.com/en-us/Abstract+Algebra>



PROJECT:-GROUP THEORY APPLICATION

STUDENTS PARTICIPATED:-

<u>NAME</u>	<u>ROLL</u>
I)SHOUNAK CHAKROBORTY	364
II)SAKIL AHAMED SARDER	347
III) PROTTUSH KR BISWAS	357
IV)TRIDEV MONDAL	359



SUPERVISED BY

PRAVANJAN KUMAR RANA

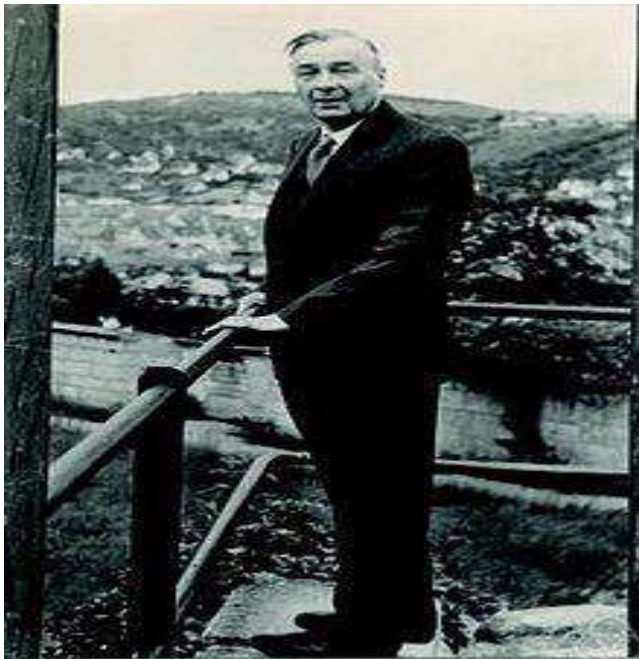
ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our respected teacher **Pravanjan Kumar Rana** who gave us the golden opportunity to do this wonderful project on **Group theory Application**. we got to learn a lot more, from this project about **hall subgroup** which will be very helpful for us.

In the end, we would like to thank our team. Without them, would not have been able to complete this project.

HALL SUBGROUP;AN APPLICATION OF SYLOW THEOREM

INTRODUCTION



Philip Hall (11 April 1904 – 30 December 1982), was an English mathematician. His major work was on group theory, notably on finite groups and solvable groups.

He was educated first at Christ's Hospital, where he won the Thompson Gold Medal for mathematics, and later at King's College Cambridge. He was elected a Fellow of the Royal Society in 1951 and awarded its Sylvester medal in 1961. He was President of the London Mathematical Society in 1955–1957, and awarded its Berwick Prize in 1958 and De Morgan Medal in 1965.

HALL SUBGROUP

In mathematics, a **Hall subgroup** of a finite group, G is a subgroup whose order is coprime to its index. They were introduced by the group theorist Phillip hall (1928).

DEFINATION

A **Hall divisor** (also called a unitary division) of an integer n is a divisor d of n such that d and n/d are coprime. The easiest way to find the Hall divisors is to write the **prime factorization** for the number in question and take any product of the multiplicative terms (the full power of any of the prime factors), including 0 of them for a product of 1 or all of them for a product equal to the original number.

For example, to find the Hall divisors of 60, show the prime factorization is $2^2 \cdot 3 \cdot 5$ and take any product of $\{3,4,5\}$. Thus, the Hall divisors of 60 are 1, 3, 4, 5, 12, 15, 20, and 60.

A **Hall subgroup** of G is a subgroup whose order is a Hall divisor of the order of G . In other words, it is a subgroup whose order is coprime to its index.

EXAMPLES

- Any Sylow subgroup of a group is a Hall subgroup.
- If $G = A_5$, the only simple group of order 60, then 15 and 20 are Hall divisors of the order of G , but G has no subgroups of these orders.
- The simple group of order 660 has two Hall subgroups of order 12 that are not even isomorphic (and so certainly not conjugate, even under an outer automorphism). The normalizer of a Sylow 2-subgroup of order 4 is isomorphic to the alternating group A_4 of order 12, while the normalizer of a subgroup of order 2 or 3 is isomorphic to the dihedral group of order 12.

HALL'S THEOREM

Hall proved that if G is a finite solvable group and π is any set of primes, then G has a Hall π -subgroup, and any two Hall π -subgroups are conjugate.

Moreover, any subgroup whose order is a product of primes in π is contained in some Hall π -subgroup.

This result can be thought of as a generalization of Sylow's Theorem to Hall subgroups, but the examples above show that such a generalization is false when the group is not solvable.

The existence of Hall subgroups can be proved by induction on the order of G , using the fact that every finite solvable group has a normal elementary abelian subgroup.

More precisely, fix a minimal normal subgroup A , which is either a π -group or a π' -group as G is π -separable.

By induction there is a subgroup H of G containing A such that H/A is a Hall π -subgroup of G/A . If A is a π -group then H is a Hall π -subgroup of G . On the other hand, if A is a π' -group, then by the Schur-Zassenhaus theorem, A has a complement in H , which is a Hall π -subgroup of G .

CONVERSE TO HALL'S THEOREM

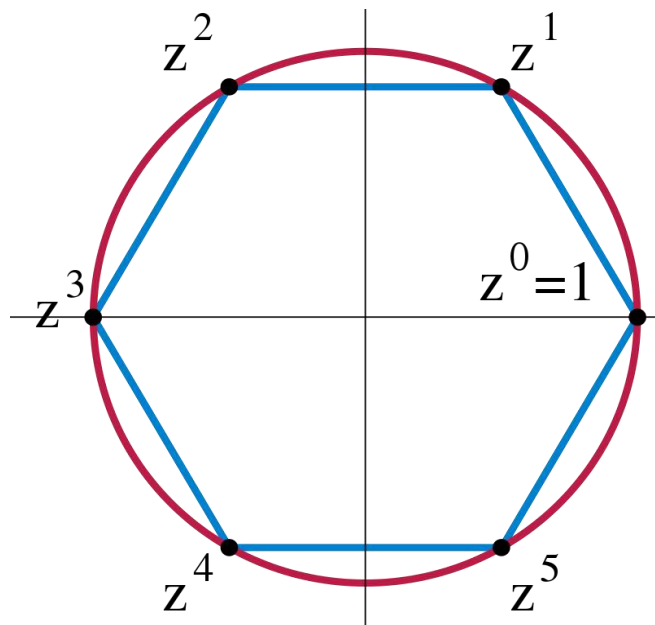
Any finite group that has a Hall π -subgroup for every set of primes π is solvable. This is a generalization of Burnside's theorem that any group whose order is of the form $p^a q^b$ for primes p and q is solvable, because Sylow's theorem implies that all Hall subgroups exist. This does not (at present) give another proof of Burnside's theorem, because Burnside's theorem is used to prove this converse.

SYLOW SYSTEMS

A **Sylow system** is a set of Sylow p -subgroups S_p for each prime p such that $S_p S_q = S_q S_p$ for all p and q . If we have a Sylow system, then the subgroup generated by the groups S_p for p in π is a Hall π -subgroup. A more precise version of Hall's theorem says that any solvable group has a Sylow system, and any two Sylow systems are conjugate.

NORMAL HALL SUBGROUP

Any normal Hall subgroup H of a finite group G possesses a complement, that is, there is some subgroup K of G that intersects H trivially and such that $HK = G$ (so G is a semidirect product of H and K). This is the Schur–Zassenhaus theorem.



REFERENCES

Gorenstein, Daniel (1980), *Finite groups*, New York: Chelsea Publishing Co.

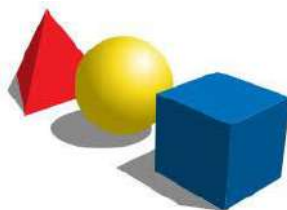
Hall, Philip (1928), "**A note on soluble groups**", **Journal of the London Mathematical Society**



PROJECT:-GROUP THEORY APPLICATION

STUDENTS PARTICIPATED:-

<u>NAME</u>	<u>ROLL</u>
I)SHOUNAK CHAKROBORTY	364
II)SAKIL AHAMED SARDER	347
III) PROTTUSH KR BISWAS	357
IV)TRIDEV MONDAL	359



SUPERVISED BY

PRAVANJAN KUMAR RANA

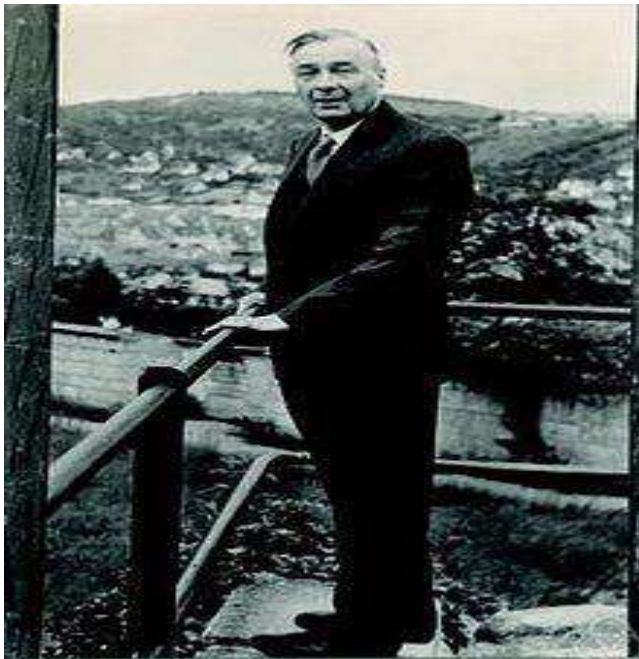
ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our respected teacher **Pravanjan Kumar Rana** who gave us the golden opportunity to do this wonderful project on **Group theory Application**. we got to learn a lot more, from this project about **hall subgroup** which will be very helpful for us.

In the end, we would like to thank our team. Without them, would not have been able to complete this project.

HALL SUBGROUP;AN APPLICATION OF SYLOW THEOREM

INTRODUCTION



Philip Hall (11 April 1904 – 30 December 1982), was an English mathematician. His major work was on group theory, notably on finite groups and solvable groups.

He was educated first at Christ's Hospital, where he won the Thompson Gold Medal for mathematics, and later at King's College Cambridge. He was elected a Fellow of the Royal Society in 1951 and awarded its Sylvester medal in 1961. He was President of the London Mathematical Society in 1955–1957, and awarded its Berwick Prize in 1958 and De Morgan Medal in 1965.

HALL SUBGROUP

In mathematics, a **Hall subgroup** of a finite group, G is a subgroup whose order is coprime to its index. They were introduced by the group theorist Phillip hall (1928).

DEFINATION

A **Hall divisor** (also called a unitary division) of an integer n is a divisor d of n such that d and n/d are coprime. The easiest way to find the Hall divisors is to write the **prime factorization** for the number in question and take any product of the multiplicative terms (the full power of any of the prime factors), including 0 of them for a product of 1 or all of them for a product equal to the original number.

For example, to find the Hall divisors of 60, show the prime factorization is $2^2 \cdot 3 \cdot 5$ and take any product of $\{3,4,5\}$. Thus, the Hall divisors of 60 are 1, 3, 4, 5, 12, 15, 20, and 60.

A **Hall subgroup** of G is a subgroup whose order is a Hall divisor of the order of G . In other words, it is a subgroup whose order is coprime to its index.

EXAMPLES

- Any Sylow subgroup of a group is a Hall subgroup.
- If $G = A_5$, the only simple group of order 60, then 15 and 20 are Hall divisors of the order of G , but G has no subgroups of these orders.
- The simple group of order 660 has two Hall subgroups of order 12 that are not even isomorphic (and so certainly not conjugate, even under an outer automorphism). The normalizer of a Sylow 2-subgroup of order 4 is isomorphic to the alternating group A_4 of order 12, while the normalizer of a subgroup of order 2 or 3 is isomorphic to the dihedral group of order 12.

HALL'S THEOREM

Hall proved that if G is a [finite solvable group](#) and π is any set of primes, then G has a [Hall \$\pi\$ -subgroup](#), and any [two Hall \$\pi\$ -subgroups](#) are conjugate.

Moreover, any subgroup whose order is a product of primes in π is contained in some [Hall \$\pi\$ -subgroup](#).

This result can be thought of as a generalization of [Sylow's Theorem](#) to [Hall subgroups](#), but the examples above show that such a generalization is false when the group is not solvable.

The existence of [Hall subgroups](#) can be proved by [induction](#) on the order of G , using the fact that every [finite solvable group](#) has a normal elementary [abelian subgroup](#).

More precisely, fix a minimal [normal subgroup](#) A , which is either a π -group or a π' -group as G is π -separable.

By [induction](#) there is a [subgroup](#) H of G containing A such that H/A is a [Hall \$\pi\$ -subgroup](#) of G/A . If A is a π -group then H is a Hall π -subgroup of G . On the other hand, if A is a π' -group, then by the [Schur-Zassenhaus theorem](#), A has a complement in H , which is a Hall π -subgroup of G .

CONVERSE TO HALL'S THEOREM

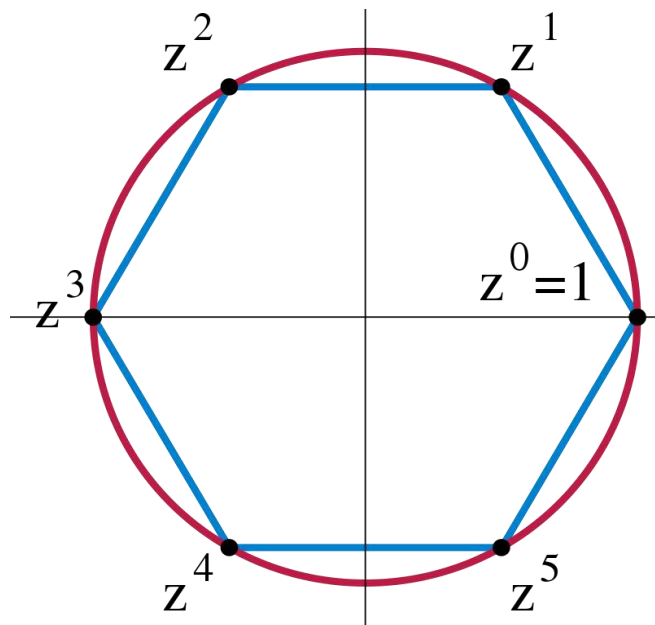
Any finite group that has a [Hall \$\pi\$ -subgroup](#) for every set of primes π is solvable. This is a generalization of [Burnside's theorem](#) that any group whose order is of the form $p^a q^b$ for primes p and q is solvable, because [Sylow's theorem](#) implies that all [Hall subgroups exist](#). This does not (at present) give another proof of Burnside's theorem, because Burnside's theorem is used to prove this [converse](#).

SYLOW SYSTEMS

A **Sylow system** is a set of Sylow p -subgroups S_p for each prime p such that $S_p S_q = S_q S_p$ for all p and q . If we have a Sylow system, then the subgroup generated by the groups S_p for p in π is a Hall π -subgroup. A more precise version of Hall's theorem says that any solvable group has a Sylow system, and any two Sylow systems are conjugate.

NORMAL HALL SUBGROUP

Any normal Hall subgroup H of a finite group G possesses a complement, that is, there is some subgroup K of G that intersects H trivially and such that $HK = G$ (so G is a semidirect product of H and K). This is the Schur–Zassenhaus theorem.



REFERENCES

Gorenstein, Daniel (1980), *Finite groups*, New York: Chelsea Publishing Co.

Hall, Philip (1928), "**A note on soluble groups**", **Journal of the London Mathematical Society**

PROJECT
on
“Group Theory”

Topic : - “Geometrical Interpretation of group Theory on Rubik's Cube”

Paper Code: MTMA CC-XII

Submitted by

Name : Arijit Majumder

Department : Mathematics

Course : B.SC

Semester : 5th

College Roll No : 1367

Exam Roll No : 2022151130

**Registration No : A01-1112-113-019-2018 of
2018-2019**

Supervised by

Prof. Pravanjan Kumar Rana

Head of the Department



Department Of Mathematics ,

Ramakrishna Misson Vivekananda Centenary College

**Akhil Mukherjee Rd, Chowdhary Para,Rahara,
Khardaha, West Bengal 700118**

Acknowledgment

As the students of mathematics of RKMVCC , I, **Arijit Majumder** are very grateful to our HOD of Mathematics department, **Prof. Pravanjan Kumar Rana** to encourage us to do this project based on the application of group theory in real world. He taught us the signification of group theory through that's what I decided to do. I learnt a lot of things from this project work. My topic is "**Geometrical Interpretation of Group Theory on Rubik's Cube**", which help us in doing a lot of Research and we came to know so many things. Since this is a group project work, I would like to thank the rest of my team members **Satyajit Roy, Supriya Pan** for helping me to complete this project work.

I would also like to thank our college for providing me all necessary resources for this project. All in all, I would like to thank everyone involved in this project and to help me with their suggestions to make the project better.

Contents

Abstract	3
1 Introduction	3
2 Rubik's Cube	4
3 Singmaster Notation	4
4 Permutation Group	5
4.1 Defination	5
5 Dihedral Group	6
6 Wreath Product	7
6.1 Defination	7
7 The Rubik's Cube Group	7
7.1 Edge Cubes	8
7.2 Corner Cubes	8
7.3 Cube Position	9
7.3.1 Example	9
7.3.2 Example	9
7.3.3 Remark	10
7.4 The Illegal Rubik's Cube Group	10
8 Fundamental Theorems of Cube Theory	10
8.1 First Fundamental Theorem of Cube Theory	11
8.2 Second Fundamental Theorem of Cube Theory	11
9 Application of the Legal Rubik's Cube Group	11
10 Sylow Theorems	12
10.1 The First Sylow Theorem	12
10.2 The Second Sylow Theorem	12
10.3 The Third Sylow Theorem	12
11 Application of Sylow Theorems on Rubik's Cube	12
12 Concluding Remarks	13
13 Reference	13

Geometrical Interpretation of Group Theory on Rubik's Cube

Supriyo Pan(1305),Arijit Majumder(1367),Satyajit Roy(320)

Abstract

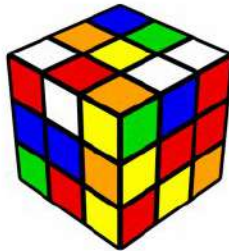
A group is a mathematical object of great importance, but the usual study of group theory is highly abstract and therefore difficult for many people to understand. A very important class of groups are so-called permutation groups which are very closely related to Rubik's cube. Thus, in addition to being a fiendishly difficult puzzle, Rubik's cube provides many concrete examples of groups and of applications of group theory. In this document, we'll alternate between a study of group theory and of Rubik's cube, using group theory to find tools to solve the cube and using the cube to illustrate many of the important topics in group theory.

1 Introduction

Invented in 1974 by Ernő Rubik, a professor of architecture living in Budapest, Hungary. now a days, the Rubik's Cube is one of the popular toys in the world. First, some quick notation. The word "cube" will usually refer to the entire cube that appears to be divided into 27 smaller cubes. We shall call these smaller cubes "cubies", of which 26 are visible. There are three types of cubies: some show only one face called "face cubies" or "center cubies", some show two faces, called "edge cubies" and some show three: the "corner cubies". The entire cube has six faces, each of which is divided into 9 smaller faces of the individual cubies. When it is important to distinguish between the faces of the large cube and the little faces on the cubies, we'll call the little faces "facelets". A permutation is a rearrangement of things. If you consider the "things" to be the facelets on Rubik's cube, it is clear that every twist of a face is a rearrangement of those facelets. Obviously, in Rubik's cube there are constraints on what rearrangements are possible, but that is part of what makes it so interesting. The three facelets that appear on a particular corner cubie, for example, will remain next to each other in every possible rearrangement. A good understanding of permutations and how they behave will help you to learn to effectively manipulate and solve Rubik's cube. The cube, however, has 54 visible facelets, so each cube movement effectively rearranges many of the 54 items. The best way to learn about any mathematical subject is to begin by looking at smaller, simpler cases. Thus in the first part of this document we'll look at permutations of small numbers of items, where we can list all the possibilities and easily keep everything in mind. When we talk about general properties of permutations in the following text, try to think about what these statements mean in the context of a few concrete examples. Rubik's cube is one such concrete example, and we'll introduce a few others as we proceed.

2 Rubik's Cube

The Rubik's Cube is a $3 \times 3 \times 3$ cube. The cube can be manipulated by rotating the faces of the cube. There are six faces, with each face composed of nine facets. On each face, the center facet is fixed, and is unmoveable. In total, there are $6 \cdot 9 = 54$ facets on the cube. Each facet is also coloured, and solving the cube requires that each face be a solid colour. That is, the nine facets of the side must all be the same colour. As well as some of the associated theorems and applications of the group. Below is a picture of what a cube looks like :

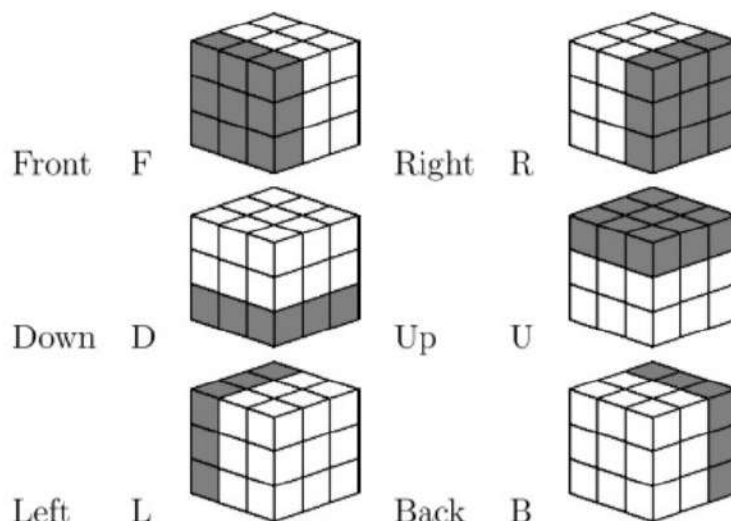


A General Puzzled Rubik's Cube

3 Singmaster Notation

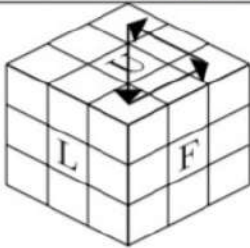
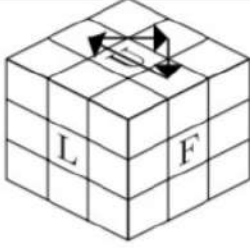
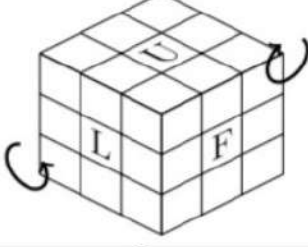
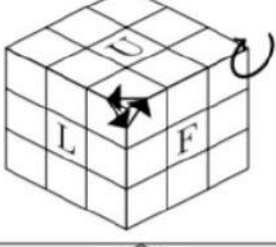
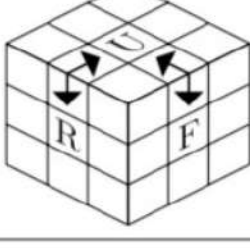
The notations are introduced by David Singmaster

- Let U denote the upward (top) face.
- Let F denote the front face.
- Let L denote the left face.
- Let R denote the right face.
- Let B denote the back face.
- Let D denote the downward (bottom) face.



The inverse of each move would be the 90 degree rotation of the face counter-clockwise and denoted by M_i^{-1} ,

where $M_i \in \{F, L, U, R, B, D\} \rightarrow$ The inverse of the combination FLU is $(FLU)^{-1}$ i.e. $U^{-1}L^{-1}F^{-1}$.

Move Sequence [1]	Diagram [6]
$RB^{-1}RF^2R^{-1}BRF^2R^2$	
$R^2UFB^{-1}R^2F^{-1}BUR^2$	
$(R^{-1}D^2RB^{-1}U^2B)^2$	
$R(U^2RF^{-1}D^2FR^{-1})^2R^{-1}$	
$LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$	

4 Permutation Group

4.1 Definition

A bijective function $\phi : A \rightarrow A$ is called permutation on A.the set

$$\mathcal{G}_A = \{ \phi \mid \phi : A \rightarrow A \text{ is a bijective function} \}$$

consisting of all permutations on A is a group with respect to the composition of functions and it is called the Permutation group on A.

To see that \mathcal{G}_A is indeed a group with respect to the composition of functions, observe that

1. If $\phi, \psi \in \mathcal{G}_A$, then obviously the composition function $\phi\psi \in \mathcal{G}_A$.
2. Since the composition is associative, thus for any $\phi, \psi, \chi \in \mathcal{G}_A$.
3. The function $I : A \rightarrow A$ defined as $I(a) = a, \forall \phi \in \mathcal{G}_A$

$$I\phi = I = \phi I$$

Thus I is identity.

4. For each $\phi \in \mathcal{G}_A, \exists$ a bijective function $\phi^{-1} : A \rightarrow A$ such that

$$\phi^{-1}\phi = I = \phi\phi^{-1}$$

Clearly, $\phi^{-1} \in \mathcal{G}_A$ and it is the inverse of ϕ .

Thus all the four conditions of a group is satisfied, hence is a group with respect to the composition of functions.

Thus given any non-empty set A , there exists a permutation group given by

$$\mathcal{G}_A = \{ \phi \mid \phi : A \rightarrow A \text{ is a bijective function} \}$$

But from now onwards we will consider only non-empty finite sets and hence will be dealing with permutation group on a finite set. Further for any finite set A of cardinality n , a one-to-one correspondance exists between the elements of A and the set $\{1, 2, 3, \dots, n\}$. Thus to study permutation group of finite sets it is enough to study the permutation groups of the sets $\{1, 2, 3, \dots, n\}$ for any positive integer n .

we denoted by S_n , the permutation group on $\{1, 2, 3, \dots, n\}$ i.e.,

$$S_n = \{ \phi \mid \phi : \{1, 2, 3, \dots, n\} \rightarrow \{1, 2, 3, \dots, n\} \}$$

The permutation group S_n is also known as the symmetric group of degree n .

5 Dihedral Group

The Dihedral group D_n is the group of symmetries of a regular polygon with n vertices. We think of this polygon as having vertices on the unit circle, with vertices labeled $0, 1, 2, \dots, n-1$ starting at $(1, 0)$ and

proceeding counterclockwise at angles in multiples of $360/n$ degrees, that is, $2\pi/n$ radians.

There are two types of symmetries of the n -gon, each one giving rise to n elements in the group D_n :

- Rotations $R_0, R_1, R_2, \dots, R_{n-1}$ where R_k is rotation of angle $2\pi k/n$.
- Reflections $S_0, S_1, S_2, \dots, S_{n-1}$, where S_k is reflection about the line through the origin and making an angle of $k\pi/n$ with the horizontal axis.

The group operation is given by composition of symmetries: if a and b are two elements in D_n , then $a \cdot b = b \circ a$. That is to say, $a \cdot b$ is the symmetry obtained by applying first a , followed by b . The elements of D_n can be thought as linear transformations of the plane, leaving the given n -gon invariant. This lets us represent the elements of D_n as 2×2 matrices, with group operation corresponding to matrix multiplication. Specifically,

$$R_k = \begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix},$$

$$S_k = \begin{pmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{pmatrix}.$$

It is now a simple matter to verify that the following relations hold in D_n :

$$\begin{aligned} R_i \cdot R_j &= R_{i+j} \\ R_i \cdot S_j &= S_{i+j} \\ S_i \cdot R_j &= S_{i-j} \\ S_i \cdot S_j &= R_{i-j} \end{aligned}$$

where $0 \leq i, j \leq n-1$ and both $i+j$ and $i-j$ are computed modulo n . The Cayley table for D_n can be readily computed from the above relations. In particular, we see that R_0 is the identity, $R_i^{-1} = R_{n-i}$ and $S_i^{-1} = S_i$.

6 Wreath Product

The product of two groups can be generalized from semi-direct products even further to wreath products. So below, we discussed the definition of Wreath product,

6.1 Definition

Let, X be a finite set, G be a group and H a group acting on X . Fix a labelling of X , say $\{x_1, x_2, x_3, \dots, x_t\}$ with $|X|=t$. Let, G^t be the direct product of G with itself 't' times. Then the wreath product of G and H is $G^t \wr H = G^t \rtimes H$, where H acts on G^t by its action on X .

7 The Rubik's Cube Group

On the Rubik's Cube, there are 54 facets that can be arranged and rearranged through twisting and turning the faces. Any position of the cube can be describe as a permutation from the solved state. Thus, the Rubik's Cube group is a subgroup of a permutation group of 54 elements.

The permutation group $G = \langle F, L, U, D, R, B \rangle \subset S_{54}$ is called the Rubik's Cube Group.

There are two different classifications of the Rubik's Cube Group that is the Legal Rubik's Cube Group and the Illegal Rubik's Cube Group. The difference between the two being that the Illegal Rubik's Cube Group allows the solver to take the cube apart and rearrange the facets. In neither case is the solver allowed to remove the stickers from each facets. As expected, the Rubik's Cube Group is a subset of the Illegal Rubik's Cube group.

Now, not all of the permutations of S_{54} will be possible on the Rubik's Cube. The middle facet on each side of the cube is fixed and cannot be permuted to a different position on the cube. Furthermore, any valid permutation on the cube will send corner facets to corner positions and edge facets to edge positions. Any other permutations will not be physically possible on the cube. Hence, G is only a subset of S_{54} and not isomorphic to the full permutation group.

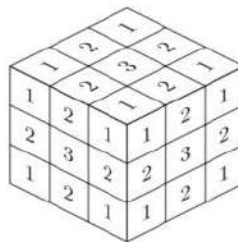


Figure 1. The different types of facets on a Rubik's Cube: 1 denotes the facets that make up corner cubes, 2 denotes facets that make up edge cubes and 3 denotes the fixed center cubes

7.1 Edge Cubes

Every edge cube in the Rubik's Cube consists of two facets, as shown in 1 and there are 12 edge cube on the Rubik's Cube. Note that for every edge cube, each of the two facets of an edge cube lie on different faces of the cube.

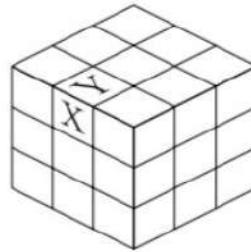


Figure 2. The 2 facets that make up an edge cube [6]

As in figure 2, facet X is on the left face and facet Y is on the upper face. Likewise, it is also possible for facets X and Y to switch places. That is, facet X would be repositioned to where facet Y is and facet Y would be moved to the position where facet X is. In terms of groups, the facets of any edge cube belong to the cyclic group of two elements C_2 . In addition, there are 12 edge cubes on the Rubik's Cube and any edge cube can occupy an edge cube spot. Thus any facet of an edge cube will be in the set $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 = 12C_2$

Likewise to describe the different arrangements of the edge cubes. There are 12 edge cubes on the Rubik's Cube and any edge cube can be in an edge cube spot. Thus, the possible arrangements of the edge cubes of the Rubik's Cube can be described by the permutation group of 12 elements, S_{12} .

(i). The position of all of the edge facets on the Rubik's Cube can be described by the group $12C_2 \wr S_{12}$

7.2 Corner Cubes

As shown in Figure 1, each corner cube consists of three facets. Now, there are a total of eight corner cubes on a Rubik's Cube and each of the facets that comprise the corner cube lie on three different sides of the cube.

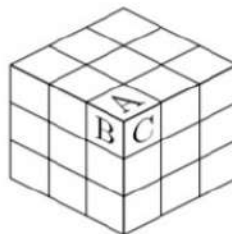


Figure 3. The 3 facets that make up a corner cube

As shown in Figure 3, facet A is on the upper face, facet B is on the left face, and facet C is on the front face. Now, it is possible to reorient the facets of a corner cube: facet A is in the position where facet B is, facet B is moved to where facet C was, facet C moved to the position of facet B; and facet A can be moved to the position of facet C, facet C to the position of facet B and facet B to the position of facet A. In terms of groups, this means that the facets of a corner cube belong

to the cyclic group of three elements C_3 . Moreover, since there are eight corner cubes, the orientation of any facet of a corner cube can be described by the set $C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 = 8_{C_3}$

7.3 Cube Position

Any corner cube be expressed as a 8-tuple and we know any edge cube position can be expressed as a 12-tuple. However, to determine the individual components of the tuples, a fixed numbering system will be needed.

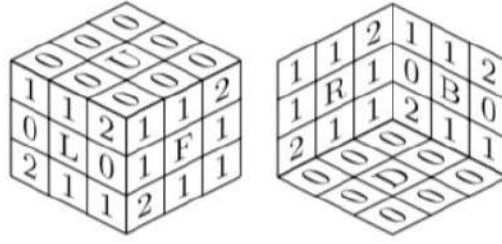


Figure 4. The fixed orientation markings, as denoted for the facets of the Rubik's Cube

For any arbitrary facet, the position of the facet is assigned the corresponding number above. Even though the facets will be moving around the cube, the numbering system remains fixed.

7.3.1 Example

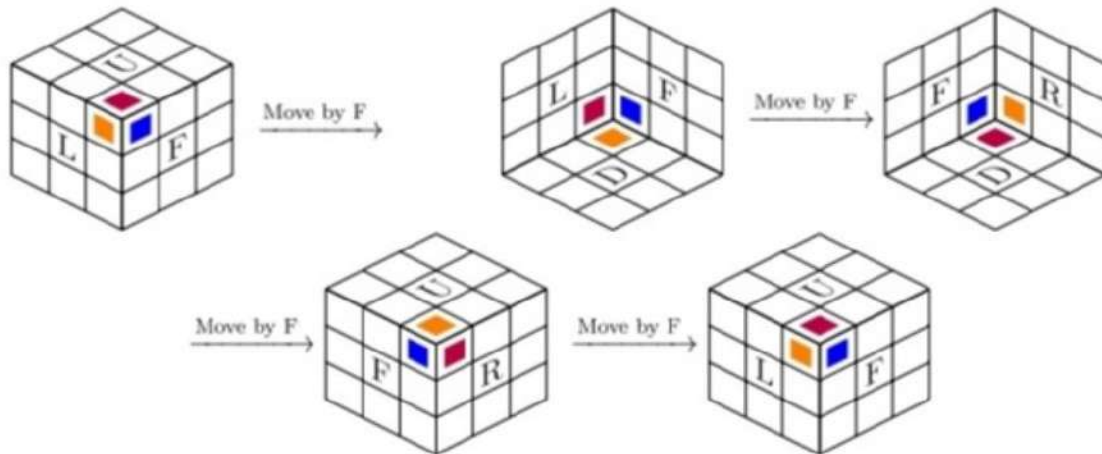
Consider the top edge cube on the front face of the Rubik's Cube [6]. It begins with a number of 1. Now, by doing the move FR, the facet is moved to the upper face on the right side. This position of the edge cube is assigned the number 0.



Figure 5. With each turn, the edge cube's orientation number is changed by either $0 \bmod 2$ or $1 \bmod 2$.

7.3.2 Example

Consider the cube below [6] and the upper, front and left face corner cube.



Tracking the blue facet, it begins with the number 1, then has number 2, number 1, number 2, and then back to number 1 to complete the cycle. Next, the purple facet starts with number 0, then goes to number 1, number 0, number 1, and then back to 0 to complete the cycle. Finally, the orange facet starts with number 2, then number 0, number 2, number 0, and then back to number 2

7.3.3 Remark

With each turn of the R; L; F or B face, the corner facet orientation number is changed by either 1 mod 3 or 2 mod 3. With each turn of the U or D face, the numbering remains unchanged (0 mod 3).

The orientation number for any facet is determined by comparing the position of the facet on the Rubik's Cube to the fixed numbering shown in Figure 4

7.4 The Illegal Rubik's Cube Group

Now, the possible arrangements of the corner cubes can be described similarly. Again, any of the eight corner cubes can occupy any of the corner cube positions of the Rubik's Cube. So, the possible arrangements of the corner cubes can be described by the permutation group of eight elements, S_8

(ii). The position of all of the corner facets on the Rubik's Cube can be described by the group $8C_3 \wr S_8$

The illegal Rubik's Cube group allows the solver to take the cube apart and reassemble it in any orientation. Again, some of the orientations are not physically possible on the cube. When all the possible positions of the facets are combined as a whole, some of the arrangements will not be physically possible on the cube.

The Illegal Rubik's Cube Group is $I = (12C_2 \wr 12) \times (8C_3 \wr S_8)$

8 Fundamental Theorems of Cube Theory

To be able to distinguish between the legal and illegal Rubik's Cube Group, the First and Second Fundamental Theorems of Cube theory are needed. The First Fundamental Theorem of Cube Theory gives the criteria for solvable arrangements of the Rubik's Cube. The illegal Rubik's Cube group allows the solver to take the cube apart and reassemble it. However, the cube may get reassembled in an arrangement that is not solvable.

8.1 First Fundamental Theorem of Cube Theory

Let, $v \in 8_{C3}, r \in S_8, w \in 12_{C2}$ and $s \in S_{12}$, then

The 4-tuple (v, r, w, s) corresponds to a arrangement(position) of the cube if and only if

- (1) $\text{sgn}(r) = \text{sgn}(s)$ (equal parity of permutations)
- (2) $v_1 + v_2 + v_3 + \dots + v_8 = 0 \pmod{3}$ (conservation of the total no of twists)
- (3) $w_1 + w_2 + w_3 + \dots + w_{12} = 0 \pmod{2}$ (conservation of the total no of flips)

8.2 Second Fundamental Theorem of Cube Theory

An operation of the cube is possible if and only if the following are satisfied:

- (1) The total number of edge and corner cycles of even length is even.
- (2) The number of corner cycles twisted right is equal to the number of corner cycles twisted left (up to modulo 3).
- (3) There is an even number of reorienting edge cycles.

9 Application of the Legal Rubik's Cube Group

Using the criteria of the First and Second Fundamental Theorems of Cube Theory, the Illegal Rubik's Cube Group can be reduced to the group

$$G_0 = \{v, r, w, s\} : v \in 8_{C3}, r \in S_8, w \in 12_{C2}, s \in S_{12}$$

where G_0 has the Properties of First and Second Cube Theorem.

The Illegal Rubik's Cube is Defined to be $I = (12_{C2} \wr 12) \times (8_{C3} \wr S_8)$

However by the conditions of the first theorem, the group is double counting some positions of the facets. The Second Condition of First Cube Theorem determines the position of the corner cubes, but note that once 7 of the corner cubes have their arrangement, the last cube's position would automatically be determined by given formula. Likewise, condition(3) determines the orientation of the cubes.

1. There exists an isomorphism $G_0 \cong (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$

$$\text{and } |G_0| = |S_8| |S_{12}| |11_{C2}| |7_{C3}| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$$

Solution : By the First Cube Theorem, The First Isomorphism Theorem of Groups and the definition of semi-direct product,

$$G_0 \cong (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12}).$$

$$|G_0| = |S_8| |S_{12}| |11_{C2}| |7_{C3}| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$$

Now to obtain the Rubik's Cube group G , G_0 must be further reduced. Condition (1) of First Cube Theory says that the number of even permutation is equal to the odd permutations. So G_0 must be further reduced by a factor of C_2

2. The Rubik's Cube Group G is the kernel of the homomorphism $\phi : G_0 \rightarrow \{1, -1\}$ so that $(v, r, w, s) \mapsto \text{sgn}(r) \text{sgn}(s)$

In particular, $G \subset G_0$ is normal of Index 2 and $|G| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$

Solution : Let, $G_0 = (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$, $H = \{1, 1\}$ and

$\phi : G_0 \rightarrow H$, where $(v, r, w, s) \mapsto \text{sgn}(r) \text{sgn}(s)$.

then $\ker(\phi) = \{v, r, w, s\} : \phi(v, r, w, s) = e_H\}$ where $e_H = 1$.

By First Cube Theorem, The First Isomorphism Theorem of Groups $G_0 / \ker(\phi) \cong G$, where $G_0 = (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$.

Next, $|G| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$ and $[G_0 : G] = (8! \cdot 12! \cdot 2^{11} \cdot 3^7) / (8! \cdot 12! \cdot 2^{10} \cdot 3^7) = 2$

10 Sylow Theorems

M.I Sylow did work of fundamental importance in determining the structure of finite groups. There are two types of groups i.e (1) Finite groups, (2) Non Finite groups. Non abelian finite groups are vastly more complicated than finite abelian groups. The Sylow Theorems are the first basic step in understanding the structure of non abelian finite groups. Since the proofs of theorems are largely unrelated to the way the theorems are actually used to analyze groups, so here I'm not giving the proofs. In this section we shall try to give this paper a sound understanding of meaning of Sylow Theorems and some examples of their application.

Throughout the general discussion in this section all groups are written multiplicatively and all integers are assumed to be nonnegative.

The main theme is the close connection between the structure of a group G and the arithmetic properties of the integer $|G|$. One of the most important results of this sort is Lagrange's Theorem, which states that if G has a subgroup H , then the order of H divides $|G|$. The First Sylow Theorem provides a particular converse.

Here, we are not discussing conjugacy class, Cauchy's theorem and p -groups because so that the paper does not get bigger.

Now we state three Sylow theorems without proof:

10.1 The First Sylow Theorem

Let G be a group of order $p^n m$ with $n \geq 1$, where p is prime, n, m are positive integers and p, m are relatively prime. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i (i is less than n) is normal in some subgroup of order p^{i+1} .

10.2 The Second Sylow Theorem

Let G be a finite group of order $p^n m$, where p is a prime, n and m are positive integers, and p and m are relatively prime. Then any two Sylow p -subgroups of G are conjugate and therefore isomorphic.

10.3 The Third Sylow Theorem

Let G be a finite group of order $p^n m$, where p is a prime, n and m are positive integers, and p and m are relatively prime. Then the number n_p of Sylow p -subgroup of G is $1 + kp$ for some nonnegative integer k and $n_p \mid m$.

11 Application of Sylow Theorems on Rubik's Cube

According to the Sylow theorems,

there exists subgroups of the cube group of the following orders: $2^{27}, 3^{14}, 5^3, 7^2, 11^1$.

That's because these are the maximal prime powers in the factorization of

$|G| = 43252003274489856000$.

Subgroups of order 11, 49, and 125 are easy to think of:

11: An 11-cycle, i.e.

$\langle (UF UL UB UR DF DL DB DR FL BL BR) \rangle$

49: Two independent 7-cycles, i.e.

$\langle (UF UL UB UR DF DL DB), (UFL UBL UBR UFR DFL DBL DBR) \rangle$

125: Three independent 5-cycles, i.e.

$\langle (UF UL UB UR DF) (DL DB DR FL BL), (UFL UBL UBR UFR DFL) \rangle$

A "3-subgroup" is also not that hard to construct, although now orientation factors in: 4 3-edge cycles, 2 3-edge cycles, 7 corners of CO freedom, which makes 3^{13} . We can also permute three orbits of three-edge-cycles among each other to get up to 3^{14} .

What I'm really wondering about is the group of order 2^{27} . I think I can get it like this (writing it out by hand to give the idea; forgive small errors):

< [Flip UF and UL],
 [Flip UF and UB],[Flip UF and UR],
 [Flip UF and DF],[Flip UF and DL],
 [Flip UF and DB],[Flip UF and DR],
 [Flip UF and FL],[Flip UF and BL], [Flip UF and BR],[Flip UF and FR],
 (UF DB),(UL DR),(UB DF),(UR DL), (FL BR),(BL FR),(UF UB)(DB DF),
 (UL UR)(DR DL),(FL FR)(BL BR), (UF UL)(DF DL)(UB UR)(DB DR), (UFL DFL)(UBL DBL)(UBR DBR)(UFL DFL), (UFL UBR),(UBL UFR),(DBR DFL), (DFR DBL),(UFL UBL)(UFR UBR), (DFL DBL)(DFR DBR) >

Which has 28 generators and gives us an illegal group whose even permutations form a subgroup of G of order 2^{27} .

Assuming I got that right, every subgroup of order 2^{27} is conjugate to that, and there are an odd number of such subgroups (Sylow theorems 2 and 3).

12 Concluding Remarks

This paper explored some of the group theory applications to the Rubik's cube and constructed the Rubik's Cube Group. The Rubik's Cube Group was shown to be

$G = \langle F, L, U, D, R, B \rangle$, which is a subgroup of S_{54} . The First and Second Fundamental Theorems of Cube Theory were presented, which gave the criteria for all the possible arrangements and moves allowed on the cube. Defined the Rubik's Cube group to

$$G = (7_{C_3} \wr S_8) \times (10_{C_2} \wr S_{12})$$

Furthermore the group G was Shown to be the kernel of homomorphism of

$$G_0 = (7_{C_3} \wr S_8) \times (10_{C_2} \wr S_{12}) \rightarrow \{1, 1\}$$

The Scope of this paper was restricted to the 3x3x3 Rubik's Cube Group; the method developed in this project can be extended to describe group structure of the 4x4x4 and 5x5x5 Rubik's Cube. Moreover, the algorithm for solving any of the 3 cubes can be described in terms of group operations.

13 Reference

- (1). Group Theory and the Rubik's Cube by Lindsey Daniels.
- (2). Group Theory, The dihedral group by Prof. Alexandru Suciu.
- (3). Group Theory, PERMUTATION GROUPS by RAJESH SINGH.
- (4). Introduction to Group Theory and Permutation puzzles.
- (5). <https://www.speedsolving.com/threads/sylow-subgroups-of-the-cube-group.20018>.
- (6). Explorations of Rubik's Cube by zeb Howell.
- (7). Thomas W. Hungerford, Abstract Algebra An Introduction (Third Edition).
- (8). D.S. Malik, John M Mordeson and M.K. Sen, Fundamentals of Abstract Algebra.



GEOMETRICAL APPROACH ON CLASS EQUATION IN GROUP THEORY

PROJECT WORK

Prepared by

Sanjay Bera

Registration no: A01-1112-113-045-2019

Examination roll no. 2022151124

Under the supervision of Dr. Pravanjan Kumar Rana

Department of Mathematics

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE, RAHARA,
KOLKATA -700118

ACKNOWLEDGEMENTS

Presentation inspiration and motivation have always played a key role in the success of my adventure.

We would like to express our special thanks of gratitude to our respected teacher Dr.P.K.Rana,H.OD. of Mathematics, Ramakrishna Mission Vivekananda Centenary College, Rahara, who gave us the golden opportunity to do this wonderful project on the topic “Geometrical Approach on Class Equation in Group Theory” which also helped me in doing a lot of research and I come to know about so many new things.

We would also like to extend our gratitude to the principle Sir Swami Kamalasthananda and Vice principle Swami Vedanuragananda for providing me with the facility that was required.

Secondly, we would also like to thank our friends who helped us a lot to finish this project within the limited time.

Last, but not the least, our parents are also an important inspiration for us so with due regards, we express our gratitude to them.

It helped us to increase our knowledge and skills.

Sanjay Bera

Date :13/01/2022

ABSTRACT: In mathematics, group theory plays a great role. Here I would like to discuss about the geometrical approach on class equation of group theory. Before dive into the topic, we see a quick overview of trough out the topic, that is see some definitions, lemmas, theorems, then entre into the main topic and at last I shall try to create a 3-D model for class equation of group. Now let's starts the journey.

INTRODUCTION: To develop my project, I need some basic definitions, some theorems, lemmas, etc. Here it is.

- A relation between nonempty sets X and Y is a subset $R \subseteq X \times Y$. We say that $x \in X$ is related to $y \in Y$ if $(x, y) \in R$. If that be the case, we shall denote it by xRy .
- Let, X be a nonempty set. A relation \sim on X is said to be an equivalence relation if it is reflexive, symmetric, transitive.

Thus, a relation \sim on X is an equivalence relation if for every $x, y, z \in X$
 (i) $x \sim x$, (ii) $x \sim y$ implies $y \sim x$ and (iii) $(x \sim y)$ and $(y \sim z)$ implies $x \sim z$.

- Suppose \sim is an equivalence relation on a nonempty set X . For $x \in X$ define $[x] := \{y \in X : x \sim y\}$

The subset $[x]$ of X is called the equivalence class of x for \sim . It is the collection of all those elements in X which are related to x for the relation \sim .

- **Lemma:** Let X be a nonempty set and \sim be an equivalence relation on X . If $y \in [x]$, then $[x] = [y]$.
- **Theorem:** Let X be a nonempty set and an equivalence relation on X . Let $x, y \in X$. Then exactly one of the following is true.
 - $[x] \cap [y] = \emptyset$.
 - $[x] = [y]$.
- A partition of a nonempty set X in a pairwise disjoint collection of subsets of X whose union is X .
- Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab . We say G is a group under this operation if the following three properties are satisfied.
 1. Associativity. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G .
 2. Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G .
 3. Inverses. For each element a in G , there is an element b in G (called an inverse of a) such that $ab = ba = e$.
- The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G . In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$.

So, now let's start the main discussion.

Let, G is a group. Then, G is a set, it is obvious. We consider a relation " R " on that set G such that $g R h \Leftrightarrow xgx^{-1}=h$, for some $x \in G$ and $g, h \in G$.

First, we have to show " R " is an equivalence relation.

- I. Let, e_G is the identity element of a group G , then for all $a \in G$ we have $e_G * a * e_G^{-1} = a$. that is $a R a$ implies " R " is a 'reflexive relation'.
- II. Let, $g, h \in G$ and $g R h$, then for some $x \in G$, we have, $x * g * x^{-1} = h$
or, $x^{-1} * (x * g * x) * x = x^{-1} * h * x$
or, $g = x^{-1} * h * x = (x^{-1}) * h * ((x^{-1}))^{-1}$
or, $h R g$ [since, $x \in G$ (group), then $x^{-1} \in G$]

Then " R " is a 'symmetric relation'.

- III. Let, $f, g, h \in G$ and $f R h$, $g R h$, then $x * f * x^{-1} = g$ and, $y * g * y^{-1} = h$, hence $y(x * f * x^{-1}) * y^{-1} = h$

Or, $f R h$, so " R " is a 'transitive relation'.

Then " R " is an "**equivalence relation**" (also known as **conjugacy relation**) on the set G (group).

Let, $a \in G$ then the *equivalence class* (also called *conjugacy class*) of that set G corresponding to that element " a " is the set $\{g \in G \mid g = x * a * x^{-1}, \text{ for some } x \in G\}$ and also denoted as $CL(a)$ or, $[a]$, that is $[a] := \{g \in G \mid g = x * a * x^{-1}, \text{ for some } x \in G\}$.

[we already know that the followings are hold, that is 1. $[g_1] = [g_2]$ or, 2. $[g_1] \cap [g_2] = \emptyset$. Where g_1, g_2 are two elements in G then one of them is hold]

Now we have, $G = \cup [a_i]$ (1)

Note that: Let, a in G such that a in $Z(G)$, then $[a] := \{g \in G \mid g = x * a * x^{-1}, \forall x \in G\}$
 $= \{g \in G \mid g = a\}$
 $= \{a\}$

Now, if, $[a] = \{a\}$, then, $g = x * a * x^{-1}, \forall x \in G$
or, $a = x * a * x^{-1}, \forall x \in G$
or, $a * x = x * a, \forall x \in G$

hence, $a \in Z(G)$, where $Z(G)$ is the center of the group G .

Now we have the result $[a] = \{a\} \Leftrightarrow a \in Z(G)$.

Or, $a \in CL(a) \Leftrightarrow a \in Z(G)$.

Note that: $Z(G) \cap [a] = \emptyset$

Now, equation (1) implies $G = Z(G) \cup CL(a_1) \cup \dots \cup CL(a_n)$, where, $o(Z(G)) = m$, i.e. for all g_i in $Z(G)$, we have $[g_i] = \{g_i\}$, $m + n = k$.

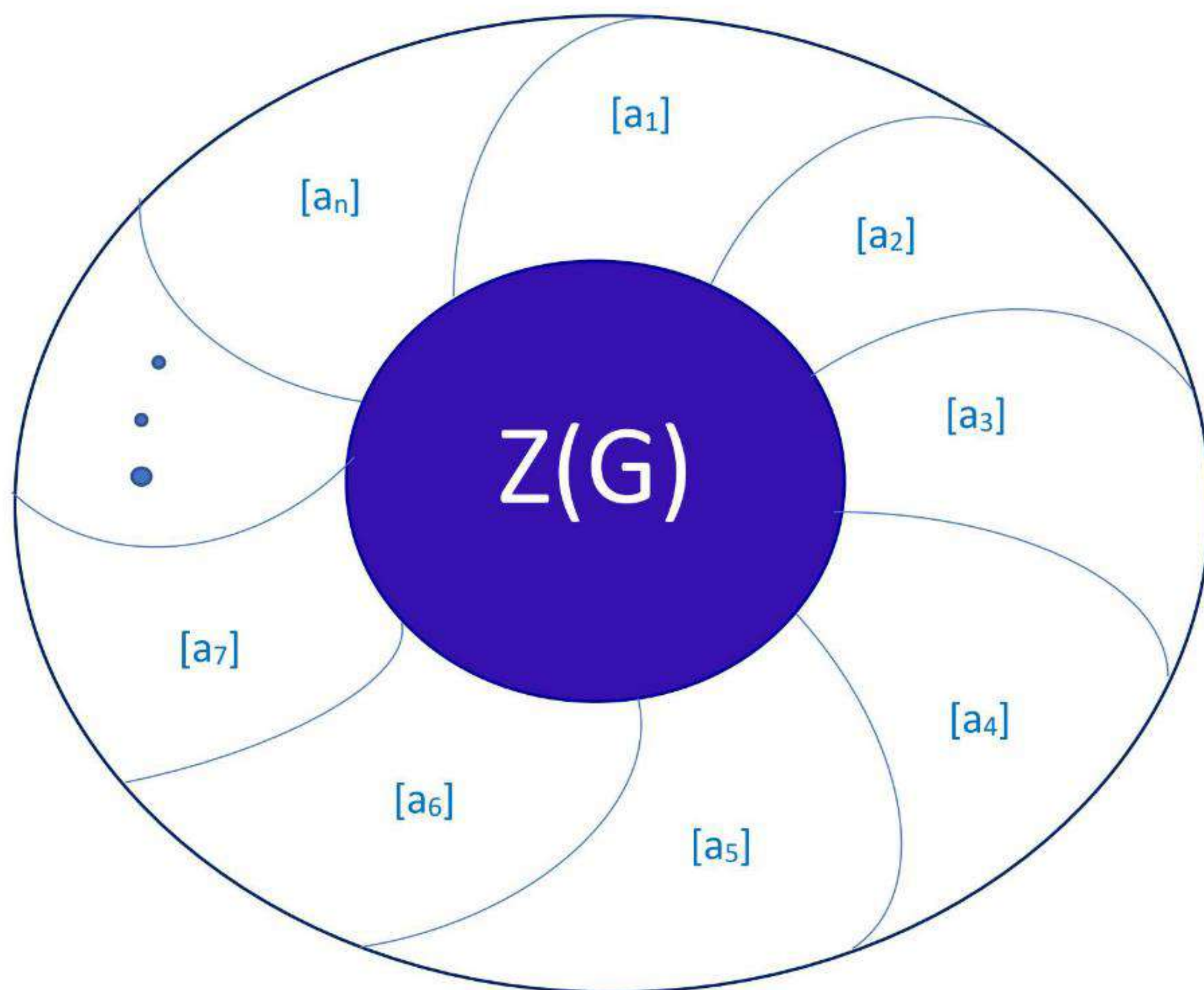
So, $O(G) = O[Z(G)] + \sum_{i=1}^n [a_i]$ (2)

Equation (2) is called the 'class equation of a finite group'.

The class equation of a finite group can also be written as $|G|=|Z(G)|+\sum_{i=1}^n[G:C(a_i)]$.

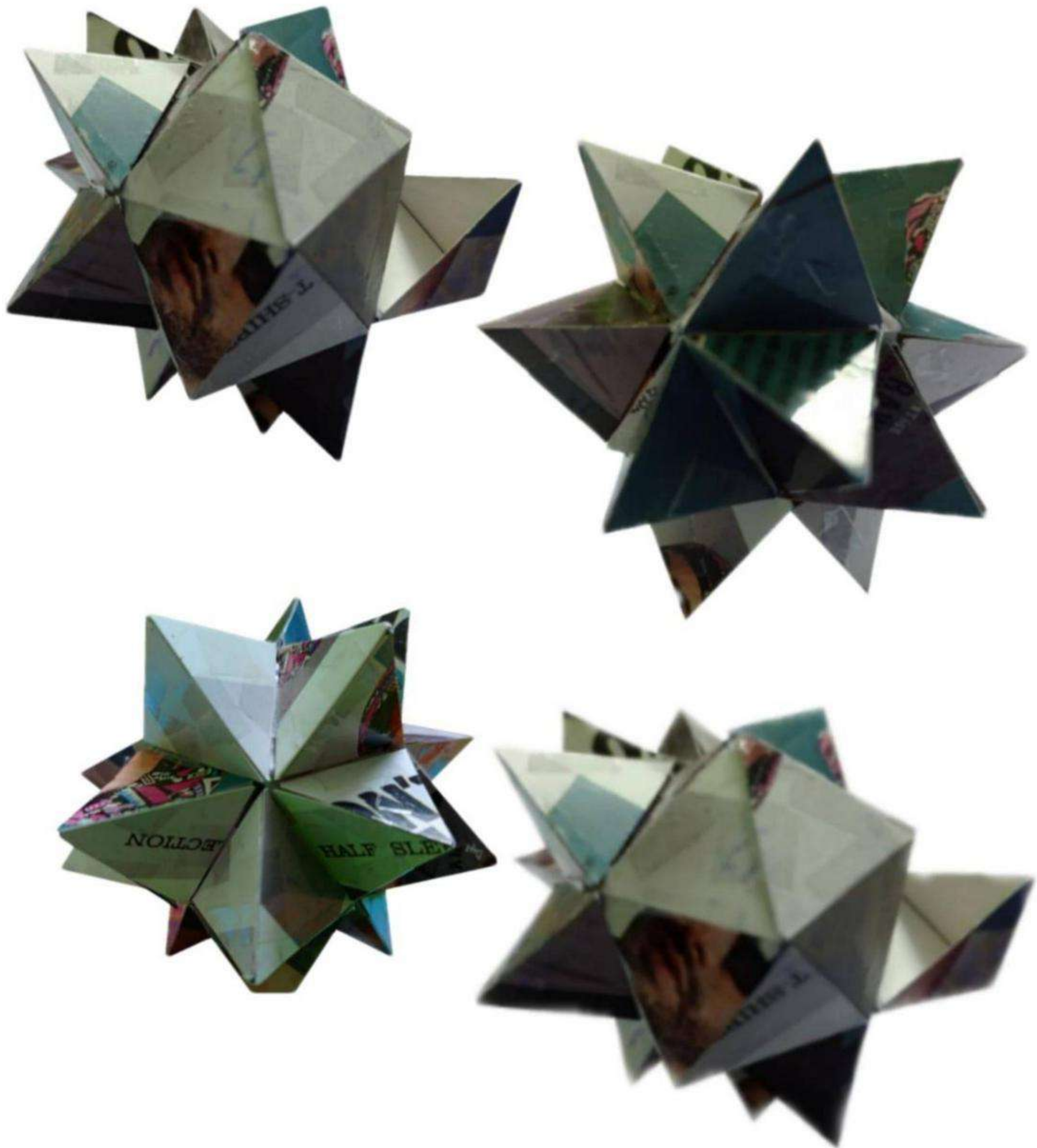
Here I try to create a diagram(2-D) of the class equation of the finite group **G**.

Here we try to create a diagram of the class equation of the finite group **G**.



[Partition of group G]

We are trying to set up a higher dimensional model for CLASS EQUATION of a GROUP(G).



REFERENCE BOOKS:

S. K. Mapa, Higher Algebra (Classical, Abstract & Linear).

M. K. Sen, S. Ghosh, P. Mukhopadhyay, Topics in Abstract Algebra.

Joseph A. Gallian, Contemporary Abstract Algebra, 4th Ed., Narosa Publishing House, New Delhi, 1999

CONCLUSION: I enjoyed this project very much, because in that field of mathematics there are so many abstract concepts, and also heart touching experiences, there are no end points of abstract algebra, since I believe that so many beautiful things also be found in future.

Project work
Submitted for partial fulfillment of the B. Sc Degree
in Mathematics

By

Soubhik Mandal



Under the supervision of **Dr. Pravanjan Kumar Rana**

Soubhik Mandal

Reg. No.: - A01-1122-113-034-2019

Examination Roll no: - 2022151117

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata- 700118

ACKNOWLEDGEMENT

*I would love reveal remarkable and extra special thanks to **Dr. Pravanjan Kumar Rana**, head of the department mathematics of RKMVCC Rahara, who gave me a very good opportunity to work on this project and with that his helpful behaviour helps me to complete this project.*

*I would also love to thank my group partners (**Raj Das and Suman parui**) who helped me a lot on this project.*

“Visual Interpretation of Sylow’s Theorem”

Key highlights: -

- *Introduction*
- *Sylow’s Theorem with visual interpretation*
- *Conclusion*
- *References*

INTRODUCTION

*The **Sylow’s theorems** are important tools in finite group theory. The **Lagrange’s theorem** tells us that the order of a subgroup of a finite group is a*

divisor of the order of that group. The converse, however, is false. There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. The most basic and widely used, is a classic theorem due to the **Norwegian mathematician Sylow**.

There are three proofs of this result of Sylow. The **first** is a very elegant and elementary argument due to **Wielandt**. It appeared in the journal *Archiv der Mathematik*, vol. 10 (1959), pages 401-402. The basic elements in Wielandt's proof are number-theoretic and combinatorial. It has the advantage, aside from its elegance and simplicity, of producing the subgroup we are seeking. The **second** proof is based on an exploitation of induction in an interplay with the **class equation**. It is one of the standard classical proofs, and is a nice illustration of the combining many of the ideals developed so far to derive this very important cornerstone due to Sylow. The **third** proof is of a completely different philosophy. The basic idea there is to show that if a larger group than the one we are considering satisfies the conclusion of the Sylow's theorem, then our group also must. This forces us to prove Sylow's theorem for a special family of groups—the symmetric groups. By invoking Cayley's Theorem, we are then able to deduce Sylow's theorem for all finite groups. Apart from this strange approach—to prove something for a given group, first prove it for a much larger one—this third proof has its own advantages. Exploiting the ideas used, we easily derive the so-called **second and third parts** of Sylow's theorem. Here we discuss about the classical proof of Sylow's theorem with **visual interpretation**.

Sylow's Theorem with Visual Interpretation

If G is a Finite group of order n and if H is a subgroup of G , then we know by Lagrange's theorem that the order of H divides n . Sylow's Theorem gives the

answer to the question, "If m is a positive integer, which divides n , does G contain a subgroup of order m ?"

Definition:(p -groups, p -subgroups): A p -group is a group whose order is a power of a prime p , A p -group that is a subgroup of group G is called **p -subgroup** of G .

For example, D_4 is a 2-group, because its order is 8, a power of the prime 2.

Two important theorems about p -groups:

Theorem 1: If a p -group G acts on a set S , then the order of S and the number of stable elements in S are congruent mod p .

Theorem 2: If H is a p -subgroup of G , then $[N_G(H):H] \equiv_p [G:H]$

- **Sylow's First Theorem:** Let G be a finite group of order $p^r m$, where p is a prime, r and m are positive integers, and p and m are relatively prime. Then G has a subgroup of order p^k for all k , $0 \leq k \leq r$.

The First Sylow Theorem generalizes **Cauchy's Theorem** [If p is a prime number that divides $O(G)$, then G has an element g of order p , and therefore a subgroup $\langle g \rangle$ of order p .] in several ways, summarized in Table 1, its proof deals with both statements in the theorem at once by using Cauchy's Theorem to expand smaller p -subgroup to create larger ones. The First Sylow tells us a bit about the relationship among p -subgroups, but we will learn more about that relationship from Second Sylow Theorem.

Proof.

It is easy to find a p -subgroup of order 1 (which is p^0) because it is obviously

Cauchy's Theorem	First Sylow Theorem
If p divides $O(G)$, then there is a subgroup of order p .	If p^i divides $o(G)$, then there is a subgroup of order p^i .
It is cyclic and has no subgroups.	Each has subgroups of orders 1, p , p^2 , up to p^i .
There is also an element of order p .	There is not necessarily an element of order p^i .

$\{e\}$. We also know that there is a p -subgroup of order p (which is p^1) from Cauchy's Theorem (as long as $O(G) > 1$). The main job of this proof is showing the existence of the larger subgroups, by explaining how to make any $H < G$ of any order $p^i < p^n$ and expand it to create a new subgroup $H^* < G$ that contains H and is p times as large, as shown in the given figure. We can then repeatedly expand the smallest p -subgroups, creating larger ones up to size p^n .

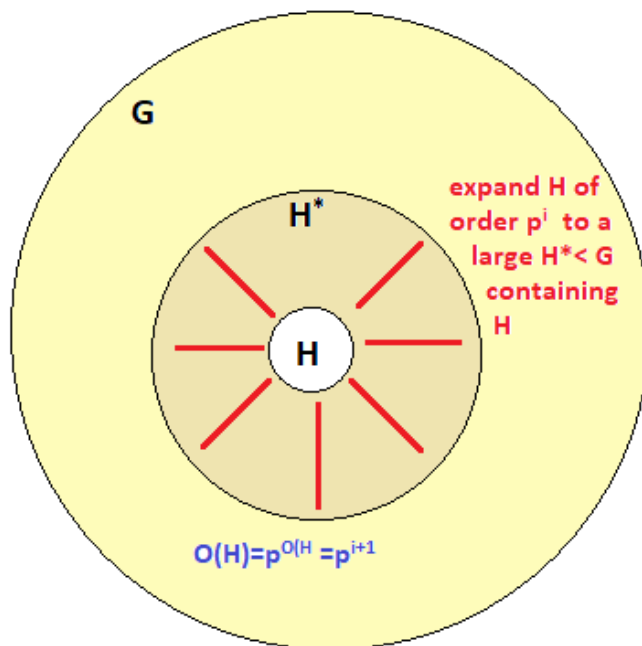


Figure: First Sylow Theorem gives a procedure for taking a subgroup of order p^i and finding a larger subgroup whose order is p^{i+1} (as long as p^{i+1} divides $O(G)$).

We can find the H^* we seek inside the normalizer $N_G(H)$ by relying on the fact that $H < N_G(H)$. Next figure illustrates the groups, subgroups, and homomorphism that come into play in the rest of this proof; refer to it help **visualize** the following argument. Create the quotient group $N_G(H)/H$ and call the quotient map q . The size of the quotient group is the number of cosets of H in its normalizer, $[N_G(H):H]$, which Theorem 2 says must be congruent to $[G:H] \pmod{p}$. So, what do we know about $[G:H]$? We're given that the order of G is some multiple of p^n , say $p^n m$. So, the number of cosets of H is

$$[G:H] = O(G)/O(H) = p^n m / p^i = p^{n-i} m.$$

Because $p^i < p^n$, we know that $p^{n-i} > 1$ and so p divides $p^{n-i} m$. Therefore $[G:H]$ and $[N_G(H):H]$ are both multiples of p .

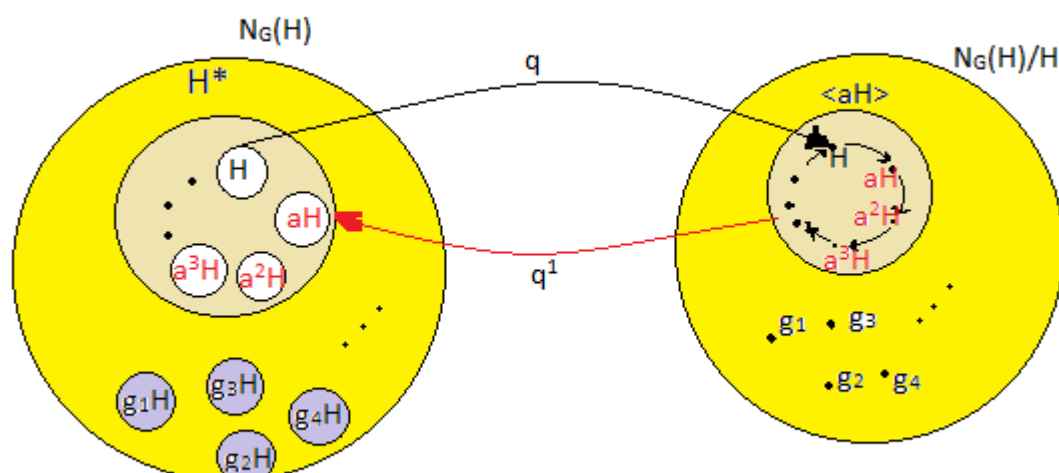


Figure: The quotient map and its inverse used in First Sylow theorem to create a subgroup H^* whose order is p times of H

The order of $N_G(H) / H$ is obviously not 0, so it must be a positive multiple of p . This lets us use Cauchy's theorem to find an element of order p in the quotient group; call that element aH . The cyclic subgroup $\langle aH \rangle$ will be very useful to us. The collection of elements that q maps to $\langle aH \rangle$ obviously contains H , but as above Figure suggests it is also a subgroup of $N_G(H)$. It is the subgroup H^* that we seek; it contains H and has size p^{i+1} for the following reason. There are p elements in $\langle aH \rangle$, and therefore p cosets of H in H^* . Since H contains p^i elements, each of its cosets does as well, and H^* contains p of them, for a total of p^{i+1} elements. The preceding paragraphs give a way to expand any H of order $p^i < p^n$ into a larger H^* of order p^{i+1} . Beginning with $H = \{e\}$, we can repeatedly expand it to create H^* , H^{**} , and so on of orders p, p^2 , up to p^n .

The expansion technique in this proof is an example of conjugacy. It applies q to H , applies Cauchy's theorem in the quotient group to turn one element into p elements, and applies q^{-1} to bring those p elements back into G , as p cosets forming a subgroup H^* . Even though q^{-1} isn't really a function, this is a useful way to summarize the argument.

Now we discuss Second and third part of Sylow's Theorem shortly:

- **The Second Sylow Theorem: Relationship among p -subgroups:**

The First Sylow Theorem guarantees the existence of subgroups of certain sizes, and what it told us of the relationship among such groups was that all smaller p -subgroups are inside larger ones. The Second Sylow Theorem shows us how the largest such p -subgroups relate through conjugacy.

Definition: (Sylow p -subgroup): We call H a Sylow p -subgroup of G if it is a p -subgroup whose order is the highest power of p that divides $O(G)$. In other words, H is a p -subgroup of G that's either the largest one, or tied for it.

Theorem:(Sylow's Second Theorem): Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then any two Sylow's p -subgroups of G are **conjugate**, and therefore **isomorphic**.

Here we mention some of its important consequences that may not at first be obvious. Conjugating by any group element creates an isomorphism from the group to itself called an inner automorphism. Thus, when two subgroups are conjugates (say $H = gKg^{-1}$), there is an inner automorphism mapping one to the other ($\Phi(x) = gxg^{-1}$). Therefore, conjugate subgroups are isomorphic. The Second Sylow Theorem tells us that all of a group's largest p -subgroups are one another's conjugates, and so they are all isomorphic to one another. Now recall the nesting relationship among p -subgroups given by the First Sylow Theorem, so that every p -subgroup is inside a Sylow p -subgroup. Conjugating any Sylow p -subgroup by any group element results in a (possibly different) Sylow p -subgroup, with identical internal structure, as shown in the Figure.

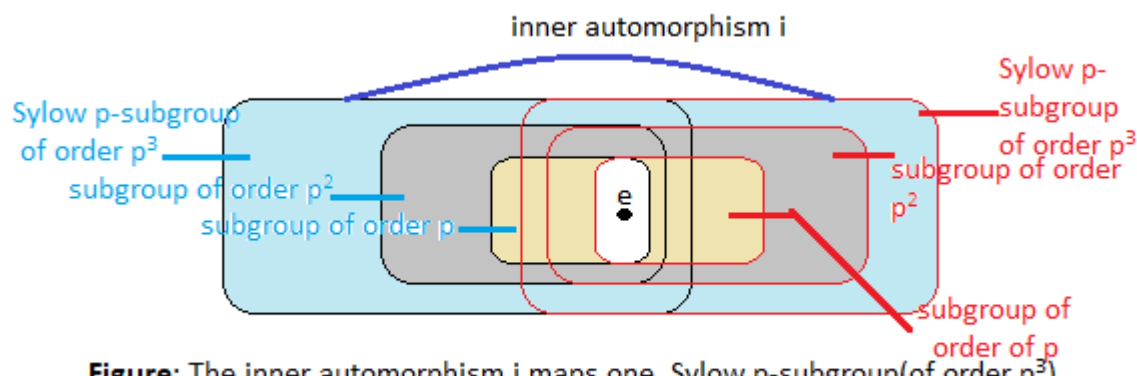


Figure: The inner automorphism i maps one Sylow p -subgroup (of order p^3) to another, which therefore has identical internal structure.

Therefore, any smaller p -subgroup must have a copy of itself (one of its conjugates) in every Sylow p -subgroup.

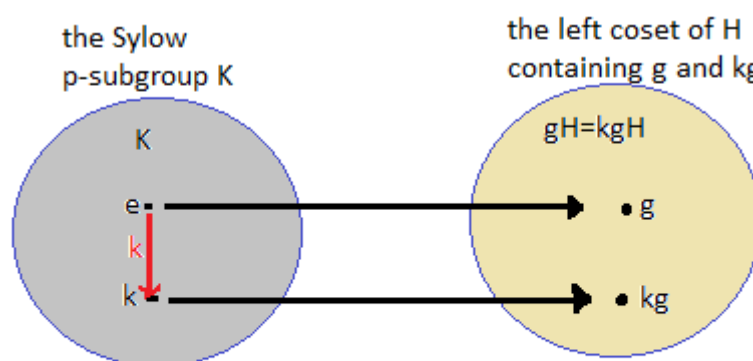


Figure: A stable element gH of the group action in the proof of the Second Sylow Theorem is one for which, for any k belong to K , $kgH = gH$.

it appears to intersect the original Sylow 2-subgroup only at the identity, that is just one possibility. For instance, if $\langle a \rangle$ were a normal subgroup, then it would be conjugate only to itself, so every Sylow 2-subgroup would contain all of $\langle a \rangle$.

- **Sylow's Third Theorem: Number of p -subgroups:**

Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then the number n_p of Sylow p Subgroups of G is $1 + kp$ for some nonnegative integer k and $n_p \mid p^r m$

This theorem helps us narrow down, just based on a group's order, the possible number of Sylow p -subgroups that the group can have.

Conclusion

The Sylow's Theorems are a powerful statement about the structure of groups in general, but are also powerful in applications of finite group theory.

Sometimes we need visualize concepts to understand the topic deeply. First, we introduce p -groups, some necessary Theorems. Then gives statement of Sylow's theorems and proof all of them with visualization. That's all from our project work.

References

- *Visual Group Theory* by Nathan C. Carter, Bentley University.
- *Topics In Algebra* by I. N. Herstein, University of Chicago.
- *Fundamentals of Abstract Algebra*, D.S. Malik (Creighton University), John M. Mordeson (Creighton University), M.K. Sen (Calcutta University).



Department of Mathematics

Akhil Mukherjee Rd, Choudhary Para,
Rahara, West Bengal 700118

PROJECT on

Symmetry Groups of the Platonic Solids

Paper Code - MTMA CC-XII

Submitted by

Name : Rittwik Banerjee
Department : Mathematics
Course : B.Sc
Semester : 5th
College Roll No : 1369
Exam Roll No : 2022151131
Registration No :
A01-1112-113-014-2018

Supervised by

Prof. Pravanjan Kumar Rana
Head of the department

Acknowledgement

With feelings of great pride and respect, we, Rittwik Banerjee & Subhrangsu Santra convey our deep sense of gratitude to our HOD of mathematics, RKMVCC, Mr. Pravanjan Kr. Rana who gave us this wonderful opportunity to work on the project 'Symmetry Groups of Platonic Solids' and also for his sincere guidance and inspiration in completing the project.

Any attempt at any level can't be satisfactorily completed without the support and guidance of parents and friends. We will always be indebted to them.

This study has indeed helped us to explore more knowledgeable avenues related to this topic and I am certain it will help us immensely in future

Content

The Tetrahedron
The Cube and Octahedron
The Dodecahedron and Icosahedron

Symmetry Groups of the Platonic Solids

Intorduction :

From the era of Ancient Greece to the modern day, five important 3-dimensional solids have captured the human imagination, playing an important role across various academic pursuits.

These five polyhedra, the Platonic Solids, have undoubtedly held a fundamental position in mathematical inquiry. From Plato's first postulation of their existence in his dialogue *The Timaeus*, to Euclid's exploration of their properties in his final book of *The Elements*—they've historically been object of mathematical interest. Still, while geometers have studied their mathematical beauty and unique symmetries for millenia , their influence isn't only limited to Mathematics. They've also played an important role in other fields. For example, in early Cosmology, Johannes Kepler used them to explore his first model of the solar system, a step towards geometric classification of planetary movements that lead to his discovery of the properties of elliptic orbits. Additionally, both Biology and Chemistry make use of their properties and symmetries, through the study of virus morphologies and the structures of the interactions of symmetric molecules respectively. Their implications don't end here; the Platonic Solids are undoubtedly important to study.

This paper serves to offer a mathematical overview of the classification of the symmetries of the Platonic Solids, determining the symmetry groups of each polyhedron explicitly.

The Tetrahedron

Proposition 1. Tetrahedra have a rotational symmetry group isomorphic to A_4 and a total symmetry group isomorphic to S_4

First, note that a tetrahedron has four vertices. For each permutation of these vertices, there exists a symmetry in the total symmetry group. Specifically, the first vertex can take four different positions. The second vertex can then end up in any of the three remaining positions via rotation. The third vertex must then take any of the final two positions by reflection, and now the position of the fourth vertex remains fixed. Therefore, under rotations and reflections, the Tetrahedron has $4 * 3 * 2 * 1$ or 24 total symmetries. Observe that the order of S_4 , the Permutation Group of order 4, also has order 24. Now, each vertex can be labeled from 1 to 4, and thus, permutations of vertex positions can be expressed under cyclic notation. Using this notation, first the rotational symmetries can be listed out. A tetrahedron has two axes of symmetry, one passing through the center of one face and the vertex right above it, and another passing through the center of one edge and the perpendicular edge adjacent to it. We can label these axes of symmetry as L and M, respectively.

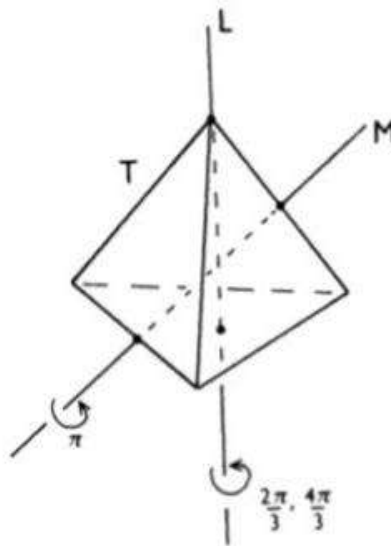


Fig : The axes of symmetry of the Tetrahedron

Clearly, an axis of type L permutes only three vertices, and thus all three cycles of the vertex elements 1, 2, 3, and 4 describe rotations along such axes. Thus, the 8 possible three cycles (123), (132), (124), (142), (134), (143), (234), and (243) correspond to the possible 120 degree symmetry rotation. On the other hand, an axis of type M permutes all four vertices, swapping them in pairs. Thus, the three possible products of two disjoint transpositions, (12)(34), (13)(24), and (14)(23) correspond to elements of the rotational symmetries wherein the solid is revolving 180 degrees. The final rotational symmetry, the identity—not rotating the shape at all—corresponds to the cyclic notation describing no permutations, (). Note that these 12 possible rotational symmetries directly correspond to all even order elements of S_4 , otherwise known as the Alternating Group A_4 . Clearly when two rotations r and r_0 prompt permutations p and p_0 respectively, their composed rotation rr_0 , prompts the permutation pp_0 , exhibiting a homomorphism. Moreover, the injective and surjective mapping explicitly listed out above exhibits a bijection. Thus, via this correspondence, the group of rotational symmetries of the Tetrahedron are isomorphic to A_4 . On a similar note, the possible reflections of the tetrahedron can also be expressed using cyclic Notation. Note that the only possible tetrahedral plane of symmetry would intersect both the midpoint of an edge and the opposite vertices of the two faces containing that edge. Equivalently, a plane of symmetry must be spanned by any two L and M axes of symmetry, and would swap any two vertices of the tetrahedron not contained in this plane. Thus all six transpositions of S_4 , (12), (13), (14), (23), (24), and (34), correspond to a reflectional symmetry. Now, the only Elements that don't correspond to a single reflection or rotation are remaining four cycles (1234), (1243), (1324), (1342), (1423), and (1432). We can see that (1234) is equivalent to the product (123)(34), and moreover, that the corresponding movement matches up with the composition of a reflection and rotation on the solid. Similarly all other elements of S_4 can be mapped to by elements generated by rotations and reflections, and this map is thus surjective. Now, as all 2 elements of S_4 map to the 24 possible rotation and reflection symmetries of the Tetrahedron, and compositions of these elements directly correspond on both sides of the mapping, the full group of symmetries is isomorphic to S_4 .

The Cube and Octahedron

Proposition 2 :Cubes and Octahedra have a rotational symmetry group isomorphic to S_4 and a total symmetry group isomorphic to $S_4 \times Z_2$ under rotational symmetries opposite vertices in a cube can be paired together, as for any rigid rotation of a vertex in a cube, its opposite vertex must move accordingly to remain opposite. Thus, in similar fashion to the argument for the number of total symmetries of a tetrahedron, we can claim that the number of rotational symmetries of a cube is the number ways you can permute these 4 pairs of vertices—if a rotation permuting all vertex couples can be found. Below, we will show that rotations do permute every vertex; it follows that the number of rotational symmetries is 24. There exist three types of axes of symmetry on the cube (Figure 4). The first type, denoted here as L, intersects the midpoint of two faces of the cube. There are three such axes, and each allows three rotational symmetries, by 90, 180, and 270 degree rotations respectively. Thus there exists nine rotations about L axes. Another axis type intersects the midpoint of two opposite edges, denoted here as M. There are six

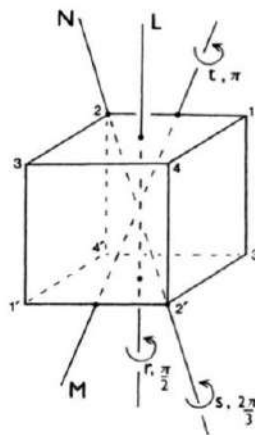


Fig : The axes of symmetry of the cube

such axes, and each has one rotational symmetry of 180 degrees, so there are 6 rotations about M axes. Finally, the last axis type, denoted here as N, intersects two

opposite vertices, and there are 4 opposite vertex pairs as previously stated. On each N axis, there are two allowed symmetries created by rotating the solid by 120 and 240 degrees. Thus, N axes have 8 allowed rotations. In sum, all possible rotations—9, 6, and 8 for each axis type—plus the identity add up to 24 symmetry element.

Using this information, it is possible to show that group of rotations above is isomorphic to S_4 . Numbering the corners on only one face of the cube from 1 to 4 allows us to then number their corresponding opposite vertices from 1' to 4' respectively, differentiating the four permutable constitute of the cube. Now, permutations of these elements directly correspond to permutations in S_4 . Note how rotation about axis types L, M, and N return four cycles, transpositions, and three cycles respectively. Additionally, observe how a product of two rotations clearly induces the correct product of two permutations in S_4 by analysis. A surjective correspondence is bijective if it maps two sets of equal size and the number of rotations found above, 24, is exactly equal to the number of elements in S_4 . Thus the group of rotations of the cube is isomorphic to S_4 . As the rotational symmetry group of the cube is isomorphic to S_4 , the rotational symmetry group of its dual, the octahedron, is also isomorphic to S_4 . Now, the full symmetry groups of a cube and an octahedron must be isomorphic to $S_4 \times \mathbb{Z}_2$

The Dodecahedron and Icosahedron

Proposition 3 : Dodecahedra and icosahedra have a rotational symmetry group isomorphic to A_5 and a total symmetry group isomorphic to $A_5 \times \mathbb{Z}_2$

First, in order to determine the number of rotational symmetries of the dodecahedron, we can count the number of ways we can permute its vertices. Note that the solid has 20 vertices, and each vertex is adjacent to 3 other vertices. Thus, there are 20 places to map our first vertex to. Taking a second vertex that was adjacent to the first vertex, there are only new 3 adjacent spots it can map to. Once two adjacent vertices are fixed, all other vertices under a rigid transformation are

then determined; the number of possible rotations of the dodecahedron is $20 * 3$ or 60. Observe that this is equal to the order of A_5 .

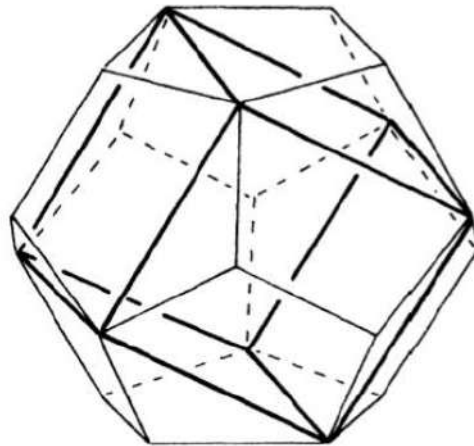


Fig : Inscribed cubes of the dodecahedron.

Similar to the way rotations permute opposite pairs of vertices of the cube as noted above, rotations of the dodecahedron permute five inscribed cubes amongst each other. Observe that the edges of each cube are diagonals of every pentagonal face of the dodecahedron. Moreover, each of the five possible diagonals on every pentagonal face corresponds to one of the five inscribed permutable cubes. We can number each cube by numbering these diagonals on the topmost face of the dodecahedron, starting at the nearest diagonal, and labeling them from 1 to 5 in a clockwise fashion—so that Figure 5 portrays the 5th diagonal and thus cube 5. Now, note that the cube has axes of symmetry that intersect opposite vertices in pairs; there are 10 such axes for the 20 vertices. Moreover, as each vertex connects three edges, and they must map to each other in a rotational symmetry about that vertex, these axes have only 2 rotational symmetry elements of 120 and 240 degrees. Therefore there are 20 total rotational symmetries among these axes, and we can show they correspond to the 20 3-cycles in A_5 . Choosing one such axes of symmetry, we can see that its rotations fix the two inscribed cubes whose N axes (as labeled in the last section, Figure 4) intersect the same two vertices. Note that the N axis has rotational symmetries of 120 and 240 degrees, equivalent to the

rotations exhibited by the dodecahedron we investigate. Now, there are three remaining inscribed cubes not-fixed by rotations by each axes of symmetry and thus must be sent to each other. These cubes can be represented by their numbered face diagonal per the labeling scheme above. Thus each rotation among these axes directly corresponds to a permutation of three cubes, or a 3-cycle in S_5 . In fact, as there exist 20 unique rotational symmetries along the 10 diagonals, 20 unique 3-cycles can be expressed. There are a total of 20 unique 3-cycles possible in S_5 , so these rotational elements must correspond to all 3-cycles in S_5 .

Finally, for $n \geq 3$ the 3-cycles generate A_n , so all the 3-cycle permutations mapped to in S_5 generate A_5 . This is clearly a homomorphism, as combination of rotations clearly correspond to associated permutation groups in A_5 by definition. Moreover, the map criteria described above details a bijection; it is surjective as all elements in A_5 could be mapped to by Theorem 6.5, and both sets have order 60 as shown at the start of this section. Thus there exists an isomorphism between A_5 and the rotational symmetry group of the dodecahedron. As the rotational symmetry group of the dodecahedron is isomorphic to A_5 , the rotational symmetry group of its dual, the icosahedron, is also isomorphic to A_5 . Now the Full Symmetry Groups of a dodecahedron and a icosahedron must be isomorphic to $A_5 \times Z_2$.

Concluding Remarks

Tetrahedra were found to have a rotational symmetry group isomorphic to S_4 . Cubes & octahedra have a rotational symmetry group isomorphic to S_4 and a total symmetry group isomorphic to $S_4 \times Z_2$. Finally dodecahedra and icosahedra have a rotational symmetry group isomorphic to A_5 and a total symmetry group isomorphic to $A_5 \times Z_2$, completing the classification of these symmetries.

References

1. M. A. Armstrong, Groups and Symmetry, Springer, New York, 1988
2. O'Connor, John, Symmetry Groups of Platonic Solids, 2003
3. Groups and Symmetry, a guide to discovering mathematics, David W. Farmer
4. Wikipedia
5. YouTube



GEOMETRICAL APPROACH ON CLASS EQUATION IN GROUP THEORY

PROJECT WORK

Prepared by

Sovon Das

Registration no: A01-1152-113-010-2019

Examination roll no. 2022151099

Under the supervision of Dr. Pravanjan Kumar Rana

Department of Mathematics

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE, RAHARA,
KOLKATA -700118

ACKNOWLEDGEMENTS

I am grateful to our respected Principal Maharaj Swami Kamalasthananda for giving us inspirations and motivation.

I am also grateful to my advisor, Dr. Pravanjan Kumar Rana (Head of the Department), Department of Mathematics, Ramakrishna Mission Vivekananda Centenary College, Rahara, Kolkata-700118 for his guidance on the related area of my project work and beautiful support.

Thanks to my parents mainly my mother to support and encourage my ideas.

Sovon Das

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College, Rahara, Kolkata-700118

Date: 07 /01/2022

ABSTRACT: In mathematics, group theory plays a great role. Here I would like to discuss about the geometrical approach on class equation of group theory. Before dive into the topic, we see a quick overview of trough out the topic, that is see some definitions, lemmas, theorems, then entre into the main topic and at last I shall try to create a 3-D model for class equation of group. Now let's starts the journey.

INTRODUCTION: To develop my project, I need some basic definitions, some theorems, lemmas, etc. Here it is.

- A relation between nonempty sets X and Y is a subset $R \subseteq X \times Y$. We say that $x \in X$ is related to $y \in Y$ if $(x, y) \in R$. If that be the case, we shall denote it by xRy .
- Let, X be a nonempty set. A relation \sim on X is said to be an equivalence relation if it is reflexive, symmetric, transitive.

Thus, a relation \sim on X is an equivalence relation if for every $x, y, z \in X$
 (i) $x \sim x$, (ii) $x \sim y$ implies $y \sim x$ and (iii) $(x \sim y)$ and $(y \sim z)$ implies $x \sim z$.

- Suppose \sim is an equivalence relation on a nonempty set X . For $x \in X$ define $[x] := \{y \in X : x \sim y\}$

The subset $[x]$ of X is called the equivalence class of x for \sim . It is the collection of all those elements in X which are related to x for the relation \sim .

- **Lemma:** Let X be a nonempty set and \sim be an equivalence relation on X . If $y \in [x]$, then $[x] = [y]$.
- **Theorem:** Let X be a nonempty set and an equivalence relation on X . Let $x, y \in X$. Then exactly one of the following is true.
 - (i) $[x] \cap [y] = \emptyset$.
 - (ii) $[x] = [y]$.
- A partition of a nonempty set X in a pairwise disjoint collection of subsets of X whose union is X .
- Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab . We say G is a group under this operation if the following three properties are satisfied.
 1. Associativity. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G .
 2. Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G .
 3. Inverses. For each element a in G , there is an element b in G (called an inverse of a) such that $ab = ba = e$.
- The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G . In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$.
- **Theorem:** Let G be a finite group of permutations of a set S . Then, for any I from S , $|G| = |\text{orb}_G(I)| \mid |\text{stab}_G(I)|$.
- **Theorem:** let G is a finite group and $a \in G$. Then $[G : C(a)] = |cl(a)|$.

So, now let's start the main discussion.

Let, G is a group. Then, G is a set, it is obvious. We consider a relation " R " on that set G such that $g R h \Leftrightarrow xgx^{-1}=h$, for some $x \in G$ and $g, h \in G$.

First, we have to show " R " is an equivalence relation.

- I. Let, e_G is the identity element of a group G , then for all $a \in G$ we have $e_G * a * e_G^{-1} = a$. that is $a R a$ implies " R " is a 'reflexive relation'.
- II. Let, g, h in G and $g R h$, then for some $x \in G$, we have, $x * g * x^{-1} = h$
or, $x^{-1} * (x * g * x) * x = x^{-1} * h * x$
or, $g = x^{-1} * h * x = (x^{-1}) * h * ((x^{-1})^{-1})$
or, $h R g$ [since, $x \in G$ (group), then $x^{-1} \in G$]

Then " R " is a 'symmetric relation'.

- III. Let, $f, g, h \in G$ and $f R h$, $g R h$, then $x * f * x^{-1} = g$ and, $y * g * y^{-1} = h$, hence $y(x * f * x^{-1}) * y^{-1} = h$

Or, $f R h$, so " R " is a 'transitive relation'.

Then " R " is an "**equivalence relation**" (also known as **conjugacy relation**) on the set G (group).

Let, $a \in G$ then the *equivalence class* (also called *conjugacy class*) of that set G corresponding to that element " a " is the set $\{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$ and also denoted as $CL(a)$ or, $[a]$, that is $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$.

[we already know that the followings are hold, that is 1. $[g_1] = [g_2]$ or, 2. $[g_1] \cap [g_2] = \emptyset$. Where g_1, g_2 are two elements in G then one of them is hold]

Now we have, $G = \cup [a_i]$ (1)

Note that: Let, a in G such that a in $Z(G)$, then $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \forall x \in G\}$
 $= \{g \in G \mid g = a\}$
 $= \{a\}$

Now, if, $[a] = \{a\}$, then, $g = x * a * x^{-1}, \forall x \in G$
or, $a = x * a * x^{-1}, \forall x \in G$
or, $a * x = x * a, \forall x \in G$

hence, $a \in Z(G)$, where $Z(G)$ is the center of the group G .

Now we have the result $[a] = \{a\} \Leftrightarrow a \in Z(G)$.

Or, $a \in CL(a) \Leftrightarrow a \in Z(G)$.

Note that: $Z(G) \cap [a] = \emptyset$

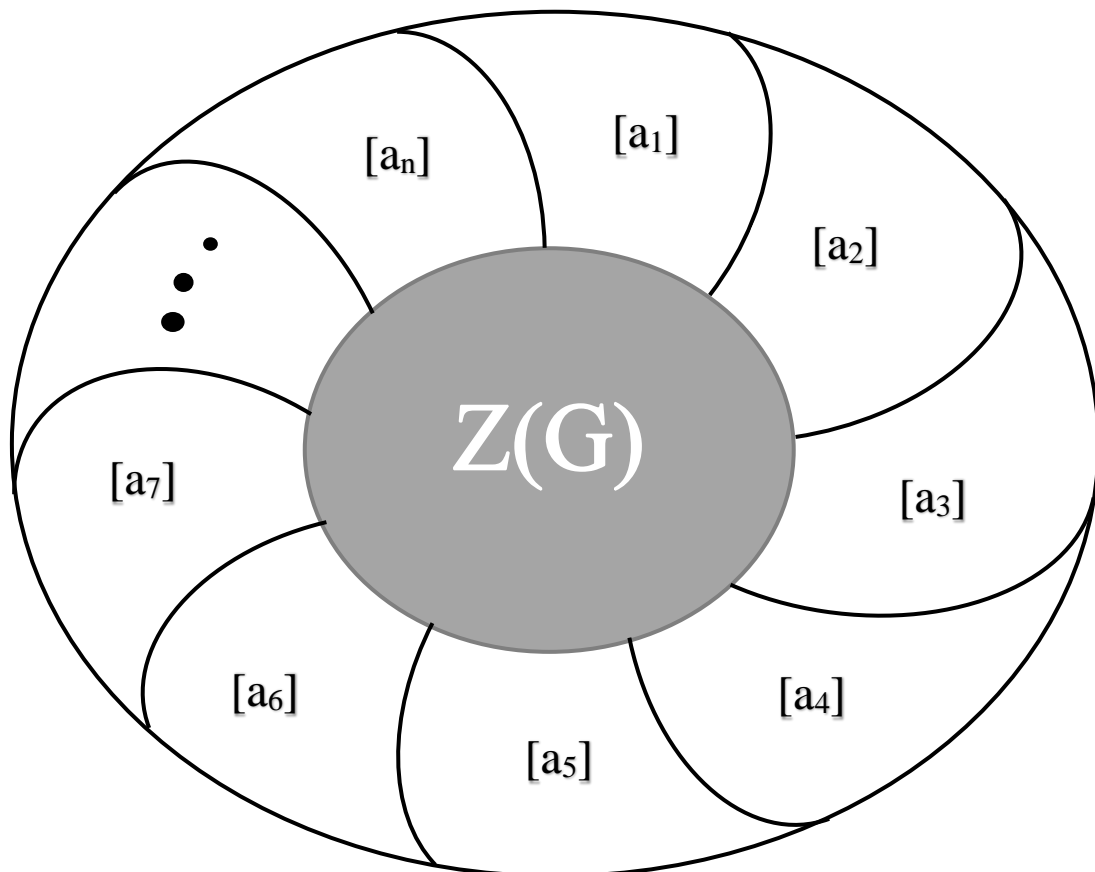
Now, equation (1) implies $G = Z(G) \cup CL(a_1) \cup \dots \cup CL(a_n)$, where, $o(Z(G)) = m$, i.e. for all g_i in $Z(G)$, we have $[g_i] = \{g_i\}$, $m + n = k$.

So, $O(\mathbf{G})=O[\mathbf{Z}(\mathbf{G})] + \sum_{i=1}^n [a_i] \dots\dots\dots(2)$

Equation (2) is called the **'class equation of a finite group'**.

The class equation of a finite group can also be written as $|G|=|Z(G)|+ \sum_{i=1}^n [G: C(a_i)]$.

Here I try to create a diagram(2-D) of the class equation of the finite group \mathbf{G} .

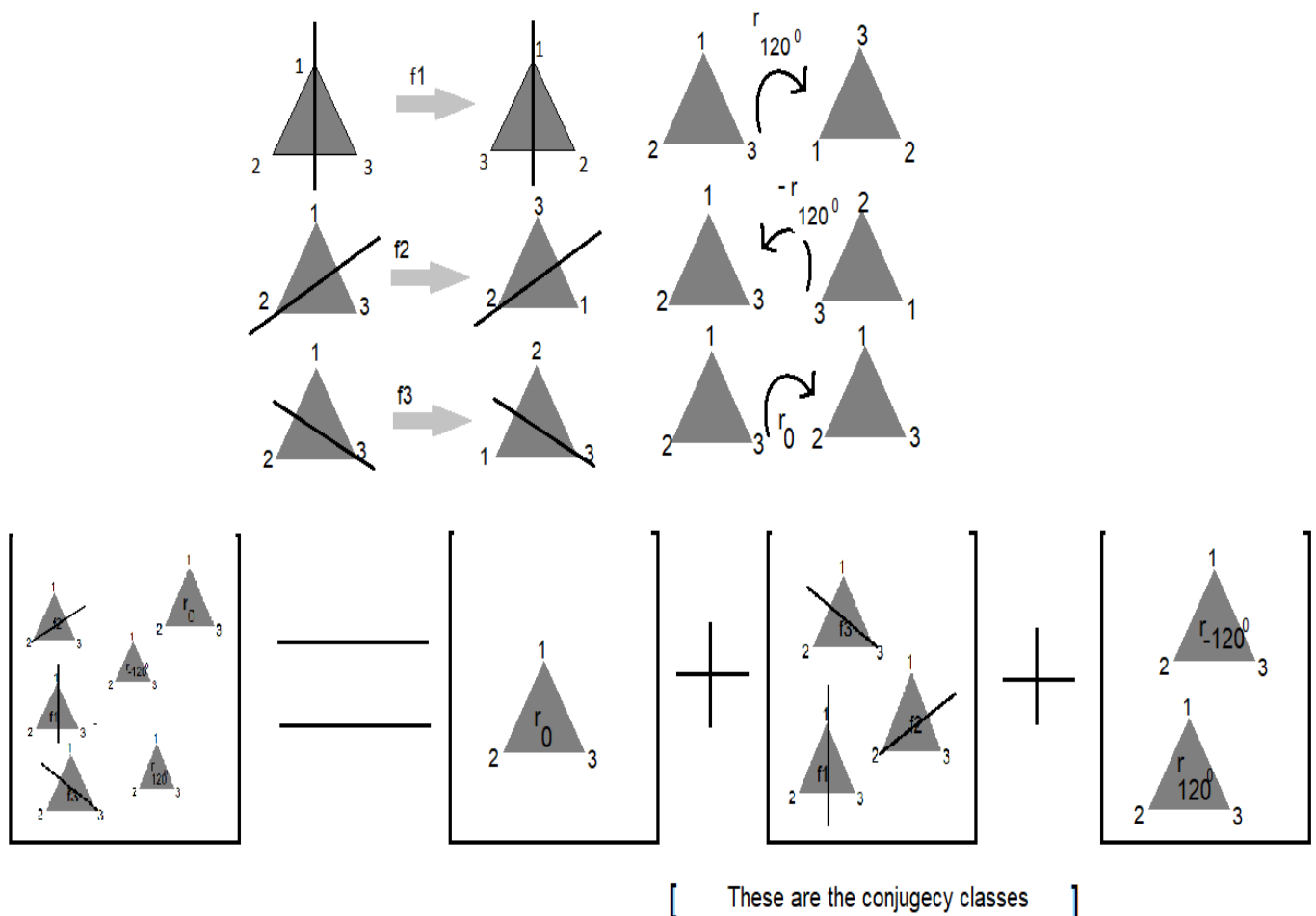


PARTITION OF A GROUP (G)

Example: Let us consider the group S_3 . The elements of S_3 are $e, (12), (23), (13), (123), (321)$. Now $\text{cl}(e) = \{e\}$, and we have $\text{cl}((12)) = \{x(12)x^{-1} \mid x \in S_3\} = \{(12), (23), (13)\}$. Similarly, $\text{cl}((123)) = \{(123), (321)\}$. Hence, $S_3 = \{e\} \cup \{(12), (13), (23)\} \cup \{(123), (321)\}$.

Then, $6 = |S_3| = |\{e\}| + |\{(12), (23), (13)\}| + |\{(123), (321)\}| = 1 + 3 + 2$, is the class equation of S_3 .

Now, I relate with the group S_3 to the symmetries of an equilateral triangle. Here it is.



References: “A Foundation Course in Mathematics”: Ajit Kumar, S. Kumaresan, Bhaba Kumar Sarma; “Topics in ABSTRACT ALGEBRA”: M K Sen, Shamik Ghosh, Parthasarathi Mukhopadhyay; “Contemporary Abstract Algebra “: Joseph A. Gallian.

Now I shall try to draw a 3-d model for class equation of a group:



Fig.(i)

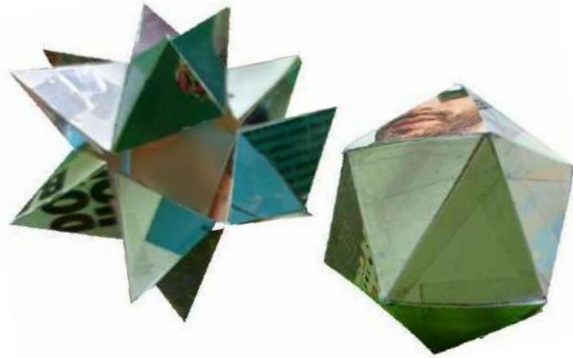


Fig.(ii)

Here, I put tetrahedrons on each faces(20) of the icosahedron ,then get that kind of symmetrical object [fig(i)], I think this represents a (all of it's symmetries) group. Now in fig(ii) I can extract this icosahedron from this group and here we see it in fig.(ii) and say that icosahedron as the centre of the group[Z(G)]. So that's why these tetrahedrons can represents the classes for that fig.(i) symmetrical object[group].

Now, let's us see quickly overview of the no of elements of icosahedron[Z(G)=G/(let)] that is also a group itself.

Ok, so let's try. In that icosahedron we see that there are 20 faces of equilateral triangles, and there are 12 vertices. We use here the Orbit-Stabilizer theorem and get that $O(G') = O(\text{Stab}(G')) * O(\text{Orb}(G')) \Rightarrow O(G') = 3 * 20 = 60$.

Let, see another photo that a center comes form the parent group, fig(iv) represents that this symmetrical object without it center,.

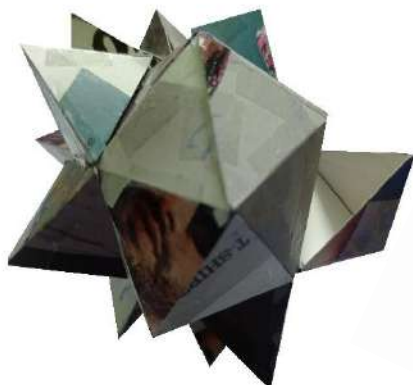


Fig.(iii)



Fig.(iv)

CONCLUTION: I enjoyed this project very much, because in that field of mathematics there are so many abstract concepts, and also heart touching experiences, there are no end points of abstract algebra, since I believe that somany beautiful things also be found in future.



GEOMETRICAL APPROACH ON CLASS EQUATION IN GROUP THEORY

PROJECT WORK

Prepared by

Mainak Mandal

Registration no: A01-1112-113-043-2019

Examination roll no. 2022151122

Under the supervision of Dr. Pravanjan Kumar Rana

Department of Mathematics

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE, RAHARA,
KOLKATA -700118

ACKNOWLEDGEMENT

Presentation inspiration and motivation have always played a key role in the success of my adventure.

We would like to express our special thanks of gratitude to our respected teacher Dr.P.K.Rana,H.OD. of Mathematics, Ramakrishna Mission Vivekananda Centenary College, Rahara, who gave us the golden opportunity to do this wonderful project on the topic “Geometrical Approach on Class Equation in Group Theory” which also helped me in doing a lot of research and I come to know about so many new things.

We would also like to extend our gratitude to the principle Sir Swami Kamalasthananda and Vice principle Swami Vedanuragananda for providing me with the facility that was required.

Secondly, we would also like to thank our friends who helped us a lot to finish this project within the limited time.

Last, but not the least, our parents are also an important inspiration for us so with due regards, we express our gratitude to them.

It helped us to increase our knowledge and skills.

Mainak Mandal

Date :13/01/2022

ABSTRACT: In mathematics, group theory plays a great role. Here I would like to discuss about the geometrical approach on class equation of group theory. Before dive into the topic, we see a quick overview of trough out the topic, that is see some definitions, lemmas, theorems, then entre into the main topic and at last I shall try to create a 3-D model for class equation of group. Now let's starts the journey.

INTRODUCTION: To develop my project, I need some basic definitions, some theorems, lemmas, etc. Here it is.

- A relation between nonempty sets X and Y is a subset $R \subseteq X \times Y$. We say that $x \in X$ is related to $y \in Y$ if $(x, y) \in R$. If that be the case, we shall denote it by xRy .
- Let, X be a nonempty set. A relation \sim on X is said to be an equivalence relation if it is reflexive, symmetric, transitive.

Thus, a relation \sim on X is an equivalence relation if for every $x, y, z \in X$
 (i) $x \sim x$, (ii) $x \sim y$ implies $y \sim x$ and (iii) $(x \sim y)$ and $(y \sim z)$ implies $x \sim z$.

- Suppose \sim is an equivalence relation on a nonempty set X . For $x \in X$ define $[x] := \{y \in X : x \sim y\}$

The subset $[x]$ of X is called the equivalence class of x for \sim . It is the collection of all those elements in X which are related to x for the relation \sim .

- **Lemma:** Let X be a nonempty set and \sim be an equivalence relation on X . If $y \in [x]$, then $[x] = [y]$.
- **Theorem:** Let X be a nonempty set and an equivalence relation on X . Let $x, y \in X$. Then exactly one of the following is true.
 - (i) $[x] \cap [y] = \emptyset$.
 - (ii) $[x] = [y]$.
- A partition of a nonempty set X in a pairwise disjoint collection of subsets of X whose union is X .
- Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab . We say G is a group under this operation if the following three properties are satisfied.
 1. Associativity. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G .
 2. Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G .
 3. Inverses. For each element a in G , there is an element b in G (called an inverse of a) such that $ab = ba = e$.
- The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G . In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$.

So, now let's start the main discussion.

Let, G is a group. Then, G is a set, it is obvious. We consider a relation " R " on that set G such that $g R h \Leftrightarrow xgx^{-1}=h$, for some $x \in G$ and $g, h \in G$.

First, we have to show " R " is an equivalence relation.

- I. Let, e_G is the identity element of a group G , then for all $a \in G$ we have $e_G * a * e_G^{-1} = a$. that is $a R a$ implies " R " is a 'reflexive relation'.
- II. Let, $g, h \in G$ and $g R h$, then for some $x \in G$, we have, $x * g * x^{-1} = h$
or, $x^{-1} * (x * g * x) * x = x^{-1} * h * x$
or, $g = x^{-1} * h * x = (x^{-1}) * h * ((x^{-1})^{-1})$
or, $h R g$ [since, $x \in G$ (group), then $x^{-1} \in G$]

Then " R " is a 'symmetric relation'.

- III. Let, $f, g, h \in G$ and $f R h$, $g R h$, then $x * f * x^{-1} = g$ and, $y * g * y^{-1} = h$, hence $y(x * f * x^{-1}) * y^{-1} = h$

Or, $f R h$, so " R " is a 'transitive relation'.

Then " R " is an "**equivalence relation**" (also known as **conjugacy relation**) on the set G (group).

Let, $a \in G$ then the *equivalence class* (also called *conjugacy class*) of that set G corresponding to that element " a " is the set $\{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$ and also denoted as $CL(a)$ or, $[a]$, that is $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$.

[we already know that the followings are hold, that is 1. $[g_1] = [g_2]$ or, 2. $[g_1] \cap [g_2] = \emptyset$. Where g_1, g_2 are two elements in G then one of them is hold]

Now we have, $G = \cup [a_i]$ (1)

Note that: Let, a in G such that a in $Z(G)$, then $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \forall x \in G\}$
 $= \{g \in G \mid g = a\}$
 $= \{a\}$

Now, if, $[a] = \{a\}$, then, $g = x * a * x^{-1}, \forall x \in G$
or, $a = x * a * x^{-1}, \forall x \in G$
or, $a * x = x * a, \forall x \in G$

hence, $a \in Z(G)$, where $Z(G)$ is the center of the group G .

Now we have the result $[a] = \{a\} \Leftrightarrow a \in Z(G)$.

Or, $a \in CL(a) \Leftrightarrow a \in Z(G)$.

Note that: $Z(G) \cap [a] = \emptyset$

Now, equation (1) implies $G = Z(G) \cup CL(a_1) \cup \dots \cup CL(a_n)$, where, $o(Z(G)) = m$, i.e. for all g_i in $Z(G)$, we have $[g_i] = \{g_i\}$, $m+n = k$.

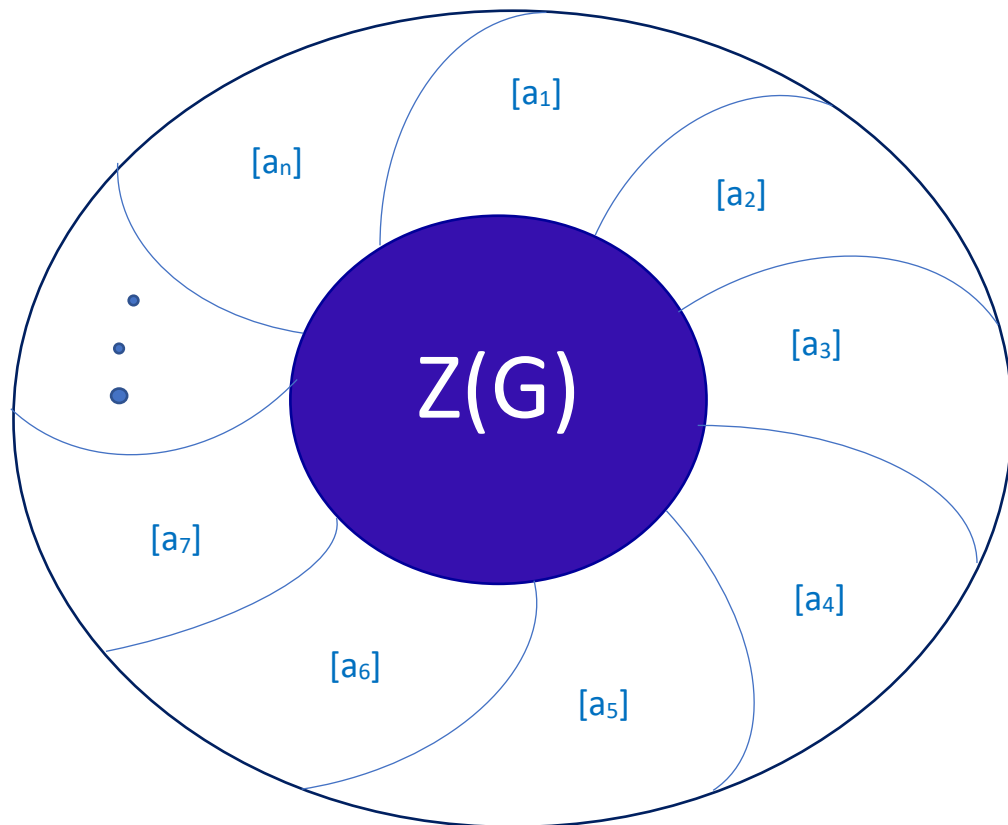
So, $O(G) = O[Z(G)] + \sum_{i=1}^n [a_i]$ (2)

Equation (2) is called the '*class equation of a finite group*'.

The class equation of a finite group can also be written as $|G|=|Z(G)|+ \sum_{i=1}^n [G: C(a_i)]$.

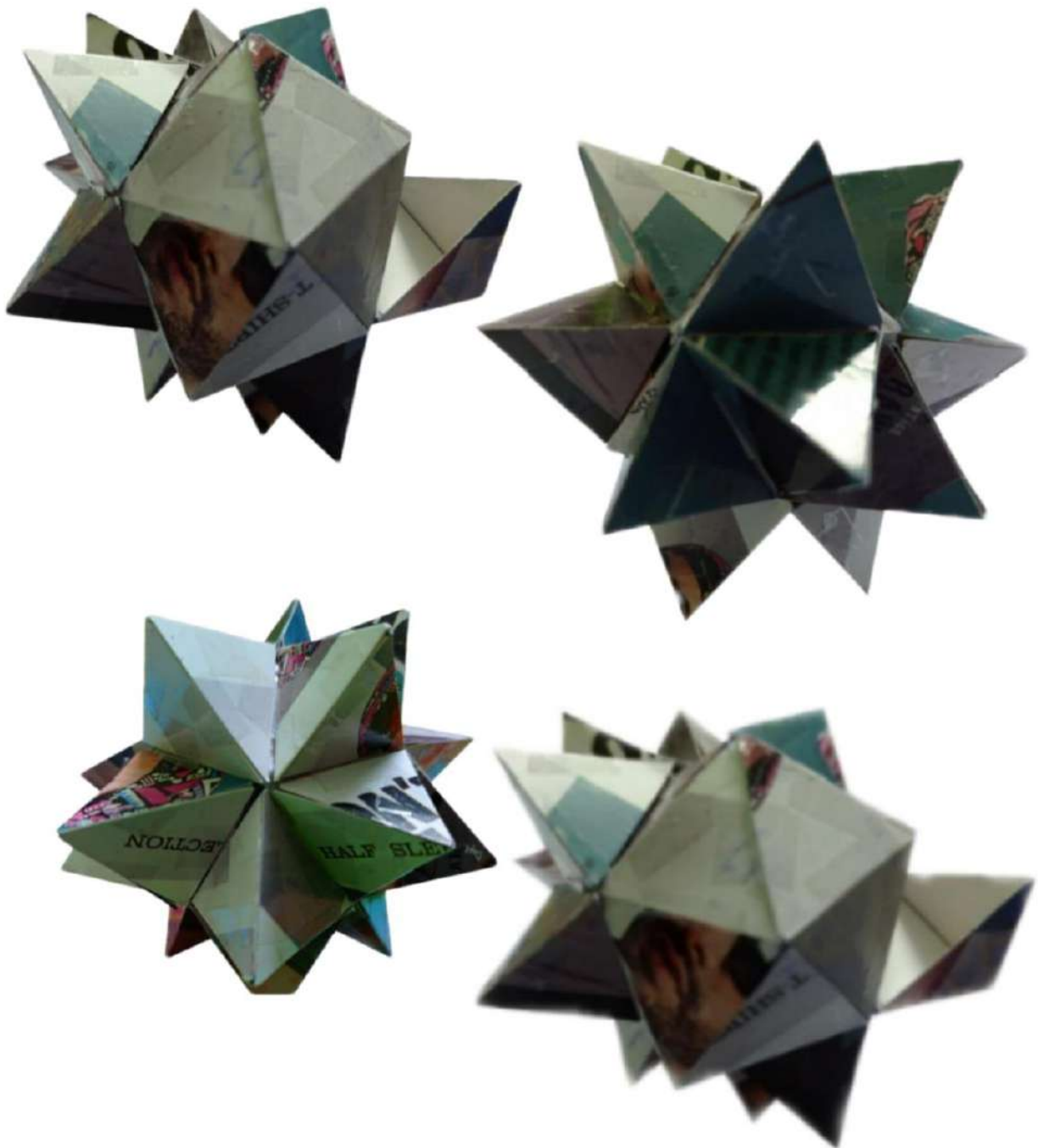
Here I try to create a diagram(2-D) of the class equation of the finite group G .

Here we try to create a diagram of the class equation of the finite group G .



[Partition of group G]

We are trying to set up a higher dimensional model for CLASS EQUATION of a GROUP(G).



REFERENCE BOOKS:

S. K. Mapa, Higher Algebra (Classical, Abstract& Linear).

M. K. Sen, S. Ghosh, P. Mukhopadhyay, Topics in Abstract Algebra.

Joseph A. Gallian, Contemporary Abstract Algebra, 4th Ed., Narosa Publishing House, New Delhi, 1999

CONCLUTION: I enjoyed this project very much, because in that field of mathematics there are so many abstract concepts, and also heart touching experiences, there are no end points of abstract algebra, since I believe that somany beautiful things also be found in future.

**RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE**



MATHEMATICS DEPARTMENT

PROJECT WORK

NAME :- AGNIVA BANERJEE

COLLEGE ROLL :- 332

REGD NO:- A01-1112-113-021-2019

EXAMINATION ROLL:- 2021151108

PAPER CODE :- MTMA CG-XII

SEMESTER :- 5th

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my advisor Prof. Peavanjan Kumar Rana , who introduced me to the wonderful project work . I would also like to thank him for the guidance , patience and help and for contributing from his abundance experience , knowledge and wisdom . It was an honour for me to get a glimpse to his world and way of thinking .My friend Sumit Paramanik and Akram Khan also helped me to do the project work , I am also thankful them.

External Direct Product and its application

Abstract:-

External direct product is one of the most important part of group theory .We are going to introduce an idea how the external direct product help us in data science , public Key Cryptography,digital signature ,genetics and electrical circuits .

Introduction:-

In this project, we show how to piece together groups to make large groups. Previously, we will show that we can often start with one large group and decompose it into a product of smaller groups in much the same way as a composite positive integer can be broken down into a product of primes. These methods will later be used to give us a simple way to construct all finite abelian groups.

Definition :

Let G_1, G_2, \dots, G_n be a finite collection of groups. The external direct product of G_1, G_2, \dots, G_n , written as $G_1 \times G_2 \times \dots \times G_n$, is the set of all n -tuples for which the i th component is an element of G_i and **the operation is component wise**.

The resulting algebraic object satisfies the axioms for a group. Specifically:

Associativity :-

The binary operation on $G \times H$ is associativity.

Identity :-

The direct product has an identity element, namely $(1_G, 1_H)$, where 1_G is the identity element of G and 1_H is the identity element of H .

Inverses :-

The inverses of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}) , where g^{-1} is the inverse of g in G , and h^{-1} is the inverse of h in H .

Hence, external direct product form a group.

In symbols, $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}$, Where $(g_1, g_2, \dots, g_n)(g_1', g_2', \dots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \dots, g_n g_n')$. It is understood that each product $g_i g_i'$ is performed with the operation of G_i . We leave it to the reader to show that the external direct product of groups is itself a group.

Properties of external direct product:-

1.Order of $(G_1 \times G_2 \times G_3 \times \dots \times G_k) = |G_1| \cdot |G_2| \cdot |G_3| \cdot \dots \cdot |G_k|$

2.The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols, $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$.

Proof : Denote the identity of G_i by e_i . Let $s = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$ and $t = |(g_1, g_2, \dots, g_n)|$. Because s is a multiple of each $|g_i|$ implies that $(g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (e_1, e_2, \dots, e_n)$, we know that $t \leq s$. On the other hand, from $(g_1, g_2, \dots, g_n)^t = (g_1^t, g_2^t, \dots, g_n^t) = (e_1, e_2, \dots, e_n)$ we see that t is a common multiple of $|g_1|, |g_2|, \dots, |g_n|$. Thus, $s \leq t$. If $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$ is an external direct product, say $(g_1, g_2, g_3, \dots, g_k) \in \text{EDP}$ Now, $(g_1, g_2, g_3, \dots, g_k)$ is just an element of $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$

Application :-

We conclude this project with five applications of the material presented here—three to cryptography, the science of sending and deciphering secret messages, one to genetics, and one to electric circuits.

Application to Data Security :-

Because computers are built from two-state electronic components, it is natural to represent information as strings of 0s and 1s called binary strings. A binary string of length n can naturally be thought of as an element of $Z_2 \times Z_2 \times \dots \times Z_2$ (n copies) where the parentheses and the commas have been deleted. Thus the binary string 11000110 corresponds to the element $(1, 1, 0, 0, 0, 1, 1, 0)$ in $Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$. Similarly, two binary strings $a_1 a_2, \dots, a_n$ and b_1, b_2, \dots, b_n are added component wise modulo 2 just as their corresponding elements in $Z_2 \times Z_2 \times \dots \times Z_2$ are. For example,

$$11000111 + 01110110 = 10110001$$

And,

$$10011100 + 10011100 = 00000000.$$

The fact that the sum of two binary sequences $a_1a_2 \dots a_n = b_1b_2 \dots b_n = 00 \dots 0$ if and only if the sequences are identical is the basis for a data security system used to protect internet transactions.

Suppose that you want to purchase a compact disc from **www.Amazon.com**. Need you be concerned that a hacker will intercept your credit-card number during the transaction? As you might expect, your credit-card number is sent to Amazon in a way that protects the data. We explain one way to send credit-card numbers over the Web securely. When you place an order with Amazon the company sends your computer a randomly generated string of 0's and 1's called a key. This key has the same length as the binary string corresponding to your credit-card number and the two strings are added (think of this process as "locking" the data). The resulting sum is then transmitted to Amazon. Amazon in turn adds the same key to the received string which then produces the original string corresponding to your credit card number (adding the key a second time "unlocks" the data).

To illustrate the idea, say you want to send an eight-digit binary string such as $s = 10101100$ to Amazon (actual credit-card numbers have very long strings) and Amazon sends your computer the key $k = 00111101$. Your computer returns the string $s + k = 10101100 + 00111101 = 10010001$ to Amazon, and Amazon adds k to this string to get $10010001 + 00111101 = 10101100$, which is the string representing your credit-card number. If someone intercepts the number $s + k = 10010001$ during transmission it is no value without knowing k . The method is secure because the key sent by Amazon is randomly generated and used only one time. You can tell when you are using an encryption scheme on a web transaction by looking to see if the web address begins with "https" rather than the customary "http." You will also see a small padlock in the status bar at the bottom of the browser window.

Application to Public Key Cryptography :-

In the mid-1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman devised an ingenious method that permits each person who is to receive a secret message to tell publicly how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message. The idea is based on the fact that there exist efficient methods for finding very large prime numbers (say about 100 digits long) and for multiplying large numbers, but no one knows an efficient algorithm for factoring large integers (say about 200 digits long). So, the person who is to receive the message chooses a pair of large primes p and q and chooses an integer r with $1 < r < m$, where $m = \text{lcm}(p - 1, q - 1)$, such that r is relatively prime to m (any such r will do). This person calculates $n = pq$ and announces that a message M is to be sent to him or her publicly as $M_r \bmod n$. Although r , n , and M_r are available to everyone, only the person who knows how to factor n as pq will be able to decipher the message. To present a simple example that nevertheless illustrates the principal features of the method, say we wish to send the message "YES." We convert the message into a string of digits by replacing A by 01, B by 02, . . . , Z by 26, and a blank by 00. So, the message YES becomes 250519. To keep the numbers involved from becoming too unwieldy, we send the message in blocks of four digits and fill in with blanks when needed. Thus, the message YES is represented by the two blocks 2505 and 1900. The person to whom the message is to be sent has picked two primes p and q , say $p = 37$ and $q = 73$ (in actual practice, p and q would have 100 or so digits), and a number r that has no prime divisors in common with $\text{lcm}(p - 1, q - 1) = 72$, say $r = 5$, and has published $n = 37 * 73 = 2701$ and $r = 5$ in a public directory. We will send the "scrambled" numbers $(2505)_5 \bmod 2701$ and $(1900)_5 \bmod 2701$ rather than 2505 and 1900, and the receiver will unscramble them. We show the work involved for us and the receiver only for the block 2505. The arithmetic involved in computing these numbers is simplified as follows:

$$2505 \bmod 2701 = 2505$$

$$(2505)^2 \bmod 2701 = 602$$

$$(2505)^4 \bmod 2701 = (602)(602) \bmod 2701 = 47$$

$$\text{So, } (2505)^5 \bmod 2701 = (2505)(47) \bmod 2701 = 2415.$$

Thus, the number 2415 is sent to the receiver. Now the receiver must take this number and convert it back to 2505. To do so, the receiver takes the two factors of 2701, $p = 37$ and $q = 73$, and calculates the least common multiple of $p - 1 = 36$ and $q - 1 = 72$, which is 72 (This is where the knowledge of p and q is necessary.) Next, the receiver must find $s = r^{-1}$ in $U(72)$ —that is, solve the equation $5 * s = 1 \bmod 72$. This number is 29. (There is a simple algorithm for finding this number.) Then the receiver takes the number received, 2415, and calculates $(2415)^{29} \bmod 2701$. This calculation can be simplified as follows:

$$2415 \bmod 2701 = 2415$$

$$(2415)^2 \bmod 2701 = 766$$

$$(2415)^4 \bmod 2701 = (766)^2 \bmod 2701 = 639$$

$$(2415)^8 \bmod 2701 = (639)^2 \bmod 2701 = 470$$

$$(2415)^{16} \bmod 2701 = (470)^2 \bmod 2701 = 2119$$

So, $(2415)^{29} \bmod 2701 = (2415)^{16} (2415)^8 (2415)^4 \bmod 2701 =$
 $(2119)(470)(639)(2415) \bmod 2701 = ((2119)(470) \bmod 2701 * (639)(2415) \bmod 2701) \bmod 2701$
 $5(1962)(914) \bmod 2701 = 52505$. [We compute the product $(2119)(470)(639)(2415)$ in two stages so that we may use a hand calculator.]

Thus the receiver correctly determines the code for "YE." On the other hand, without knowing how pq factors, one cannot find the modulus (in our case, 72) that is needed to determine the intended message.

Application to Digital Signatures :-

With so many financial transactions now taking place electronically, the problem of authenticity is paramount. How is a stockbroker to know that an electronic message she receives that tells her to sell one stock and buy another actually came from her client? The technique used in public key cryptography allows for digital signatures as well. Let us say that person A wants to send a secret message to person B in such a way that only B can decode the message and B will know that only A could have sent it. Abstractly, let E_A and D_A denote the algorithms that A uses for encryption and decryption, respectively, and let E_B and D_B denote the algorithms that B uses for encryption and decryption, respectively. Here we assume that E_A and E_B are available to the public, whereas D_A is known only to A and D_B is known only to B and that $D_B E_B$ and $E_A D_A$ applied to any message leaves the message unchanged. Then A sends a message M to B as $E_B(D_A(M))$ and B decodes the received message by applying the function $E_A D_B$ to it to obtain

$$(E_A D_B)(E_B(D_A(M))) = E_A(D_B E_B)(D_A(M)) = E_A(D_A(M)) = M.$$

Notice that only A can execute the first step [i.e., create $D_A(M)$] and only B can implement the last step (i.e., apply $E_A D_B$ to the received message).

Transactions using digital signatures became legally binding in the United States in October 2000.

Application to Genetics :-

The genetic code can be conveniently modeled using elements of $Z_4 \times Z_4 \times \dots \times Z_4$ where we omit the parentheses and the commas and just use strings of 0s, 1s, 2s, and 3s and add component wise modulo 4. A DNA molecule is composed of two long strands in the form of a double helix. Each strand is made up of strings of the four nitrogen bases adenine (A), thymine (T), guanine (G), and cytosine (C). Each base on one strand binds to a complementary base on the other strand. Adenine always is bound to thymine, and guanine always is bound to cytosine. To model this process, we identify A with 0, T with 2, G with 1, and C with 3. Thus, the DNA segment ACGTAACAGGA and its complement segment TGCATTGTCCT are denoted by

03120030110 and 21302212332. Noting that in Z_4 , $0 + 2 = 2$, $2 + 2 = 0$, $1 + 2 = 3$, and $3 + 2 = 1$, we see that adding 2 to elements of Z_4 interchanges 0 and 2 and 1 and 3. So, for any DNA segment $a_1 a_2 \dots a_n$ represented by element of $Z_4 \times Z_4 \times \dots \times Z_4$, we see that its complementary segment is represented by $a_1 a_2 \dots a_n + 22 \dots 2$.

Application to Electric Circuits :-

Many homes have light fixtures that are operated by a pair of switches. They are wired so that when either switch is thrown the light changes its status (from on to off or vice versa). Suppose the wiring is done so that the light is on when both switches are in the up position. We can conveniently think of the states of the two switches as being matched with the elements of $Z_2 \times Z_2$ with the two switches in the up position corresponding to $(0, 0)$ and the two switches in the down position corresponding to $(1, 1)$. Each time a switch is thrown, we add 1 to the corresponding component in the group $Z_2 \times Z_2$. We then see that the lights are on when the switches correspond to the elements of the subgroup $\{(1, 1)\}$ and are off when the switches correspond to the elements in the coset $(1, 0) + (1, 1)$. A similar analysis applies in the case of three switches with the subgroup $\{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$ corresponding to the lights-on situation

Conclusion:-

The role of external direct product in modern algebra cannot describe in a sentence. The use of external direct product is not only limited in group theory but also we can see the use of it in many branches of mathematics like topology and so on. If we come out from algebra then we can see that external direct product also plays a vital role in our daily life. So we can say a mathematics student should know the application of mathematics in daily life

References:-

1. John B. Fraleigh ,A first course of Abstract Algebra ,7th Ed.,pearson 2007
2. Joseph A. Gallian , Contemporary Abstract Algebra,4th Ed. Narosa Publishing House,1999
3. D.S.Malik, John M. Mordeson and M.K.Sen, Fundamental of Abstract Algebra

**RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE
RAHARA, KOLKATA:-700118**

Department of Mathematics

Semester: 5th

Core Course:-XII (Group Theory-II)

**Project Title:- BURNSIDE'S LEMMA AND IT'S
APPLICATION**

Submitted By:

Subrata Khanra (Examination Roll No:-2022151106,

Reg. No:- A01-1112-113-018-2019)

Souvik Dolai (Examination Roll No:-2022151116,

Reg. No:-A01-1122-113-033-2019)

Sayan Ghosh (Examination Roll No:-2022151127,

Reg. No:-A01-1112-113-049-2019)

Supervised By:

Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and our special gratitude to **Dr. Pravanjan Kumar Rana, Head of the department of mathematics of RKMVCC Rahara** , who gave us a golden opportunity to do this project and also provided support in completing my project work.

CONTENTS

<u>Sl. No</u>	<u>Title</u>	<u>Page No</u>
1	Abstract	1
2	Introduction	1
3	Discussion	2-4
4	Application of Burnside's Lemma	5-8
5	Conclusion	8
6	Reference	8

BURNSIDE'S LEMMA AND IT'S APPLICATION

ABSTRACT:-

Burnside's Lemma, also referred to as Orbit Counting Theorem, is a result of group theory that used to count distinct objects with respect to symmetry. It provides a formula to count the number of object, where two objects that are symmetry by rotation or reflection are not categorized as distinct.

The result of this Theorem has been extensively used, in particular to enumeration of chemical isomer compounds.

INTRODUCTION:-

Mathematics is the cradle of all creation be it a farmer or a engineer, a shopkeeper or a doctor, a scientist or a magician everyone needs mathematics in their day to day life.

In this project we show how we can solve non mathematical problems with the help of Burnside's Lemma. Now we apply this theorem to a chemistry molecule in enumeration of different chemical structure are called isomers.

DISCUSSION:-

As Burnside's Lemma is a result of group theory, we will first provide some basic definitions and notations involved in group theory that will be relevant in this paper.

Let we have a group G that acts on a set X . We illustrate the groups as the following dots inside the box.

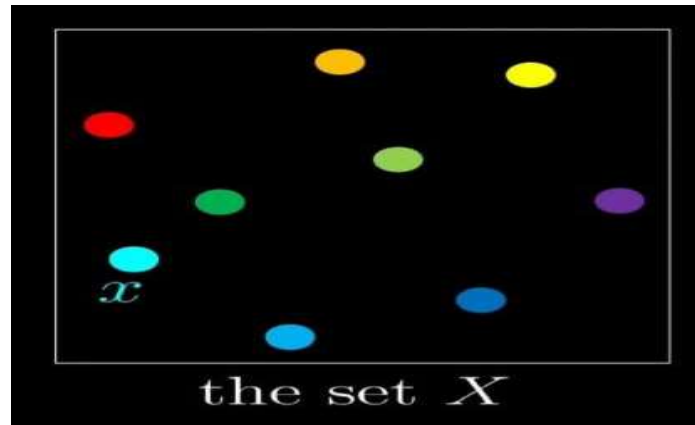


Fig:-1

Let we pick a x among the dots. Then we define its orbit where x can go under the action.

$$\text{Orbit}_G(X) = \{\text{where } x \text{ can go}\}.$$

So the elements in orbit of x are elements from the set X .

$$\text{Stab}_G(X) = \{\text{elements of } G \text{ that fixes } x\}$$

The Orbit-Stabilizer Theorem basically says that the product of the size of orbit and stabilizer of an element in X is the size of the whole group G .

We will prove Burnside's Lemma using the Orbit-Stabilizer Theorem, basically counts the number of orbits in X . We will do this using some diagram and some word as well.

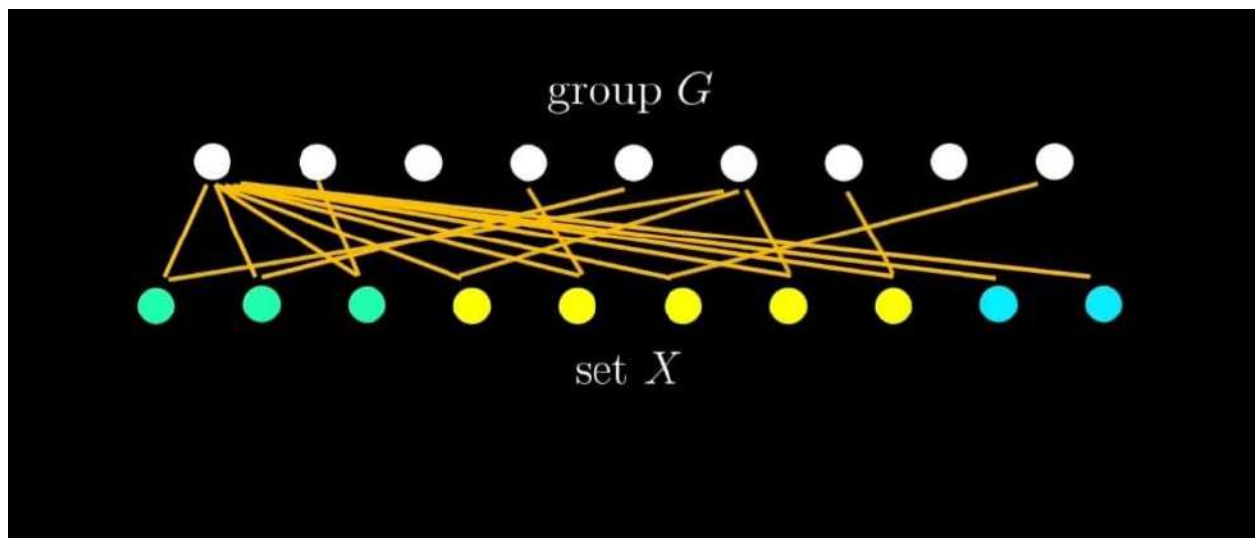


Fig:-2

In the upper picture we draw elements of G and X . Then we will draw lines from the elements of G to the elements of X . The condition of drawing the lines if $g \in G$ fixes $x \in X$ i.e. $g.x = x$ then we will draw line from g to x . The point in G marked as 1 is the identity in G .

Since identity element fixes every element in X , we have drawn lines to every element in X from the point 1.

Now we want to count the number of lines we have drawn here. From the picture we write the following table-

<u>Elements in G</u>	<u>No of lines from the elements</u>
1	10
2	1
3	0
4	1
5	1
6	3
7	1
8	0
9	1

Number in the right column of the table are the number of elements in X fixed by corresponding elements of G in left column. For example 4 fixes one elements in X .

We call the set of elements in X fixed by g in G as $\text{fix}(g)$. So the number in right columns are nothing but corresponding $|\text{fix}(g)|$. Therefore the sum $\sum_{g \in G} \text{fix}(g)$ is nothing but the number of total lines.

Now we will count again the number of lines but this time in a different way.

Let's see the lines from the lower row of figure 1 i.e. the elements of X . The collection of elements of X marked with second lying bracket are elements of same orbits. A line from $x \in X$ is drawn if g fixes x i.e. $g \in \sum_G \text{Stab}(x)$.

So the number of lines drawn from a point x in X is precisely the size of stabilizer of x that is $|\text{Stab}_G(X)|$.

Now by the Orbit-Stabilizer Theorem for any a in X

$$|\text{stab}_G(a)| = |G|/|\text{Orb}_G(a)|$$

Since order of orbit for each element in same orbit is same, we conclude that order of Stab of each element in same orbit is also same.

Therefore the total number of lines drawn from an orbit is give a number of lines drawn from one element X number of elements in the orbit, that is $|\text{Stab}_G(X)| * |\text{Orbit}_G(X)|$ that is nothing but $|G|$.

Therefore the total number of lines drawn from elements of X is the number of lines drawn from each orbit = (number of orbit) * $|G|$. Since the number of line cannot be different due to variations in counting, we have

$$(\text{Number of orbit}) * |G| = \sum_{g \in G} \text{fix}(g)$$

$$\text{So, Number of orbit} = 1/|G| * \sum_{g \in G} |\text{fix}(g)|$$

This is the awaited Burnside's Lemma.

APPLICATION OF BURNSIDE'S LEMMA

Burnside's Lemma has variety of application that has been adapted to many different fields of study. The most widely known application is within chemical isomer enumeration.

Chemical isomer enumeration:-

In chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecule in space. The molecules that have the same chemical formula but different chemical structures are called isomers, and we can use Burnside's Lemma to enumerate these type of isomers.

Let's look at an example,

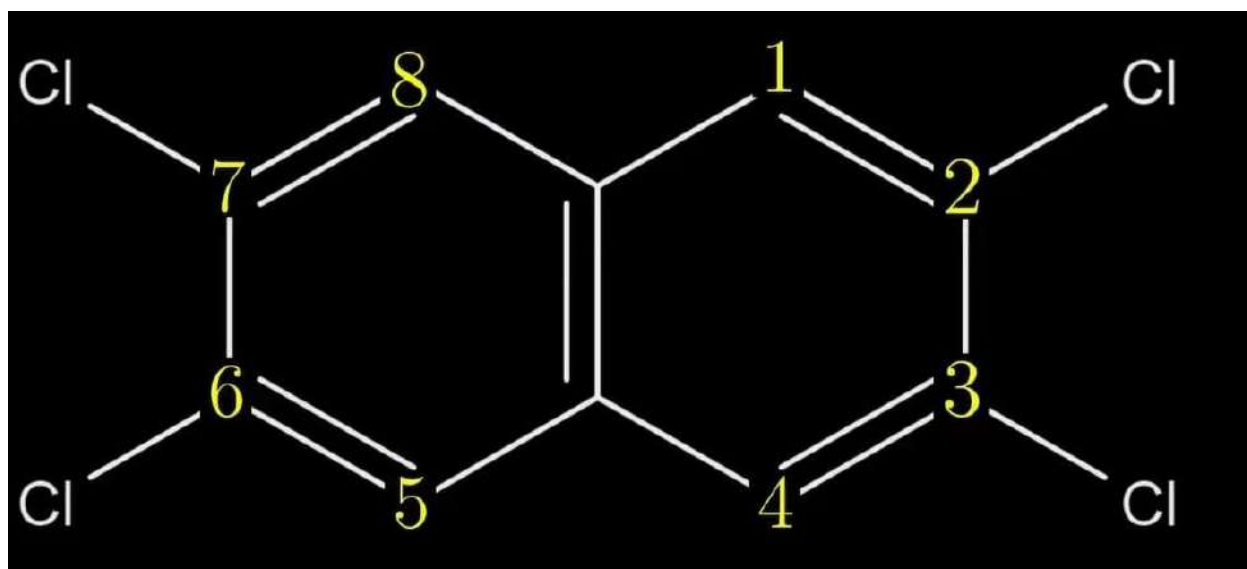


Fig:-Tetrachloronaphthalene

Now, our question is –

How much naphthalene with 4 chlorine (Cl) substituent?

We can use Burnside's Lemma to determine the required number. Here we consider four symmetries-

- ❖ Identity
- ❖ Horizontal reflection
- ❖ Vertical reflection
- ❖ 180° rotation

Burnside's Lemma: $\# \text{ Of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$

We can substitute the size of the group $|G|=4$

- First we consider the fix elements of the identity. By definition, identity fixes everything. Out of the total eight positions in naphthalene, we can choose only four different sites in the molecules where we can substitute one H by chlorine (Cl).
So its fix size = 8C_4
- Now we consider the fix size for the horizontal reflection. In this symmetry, 1 is swapped with 4, so the same thing. That is both must have the chlorine (Cl) or both not having the chlorine (Cl).

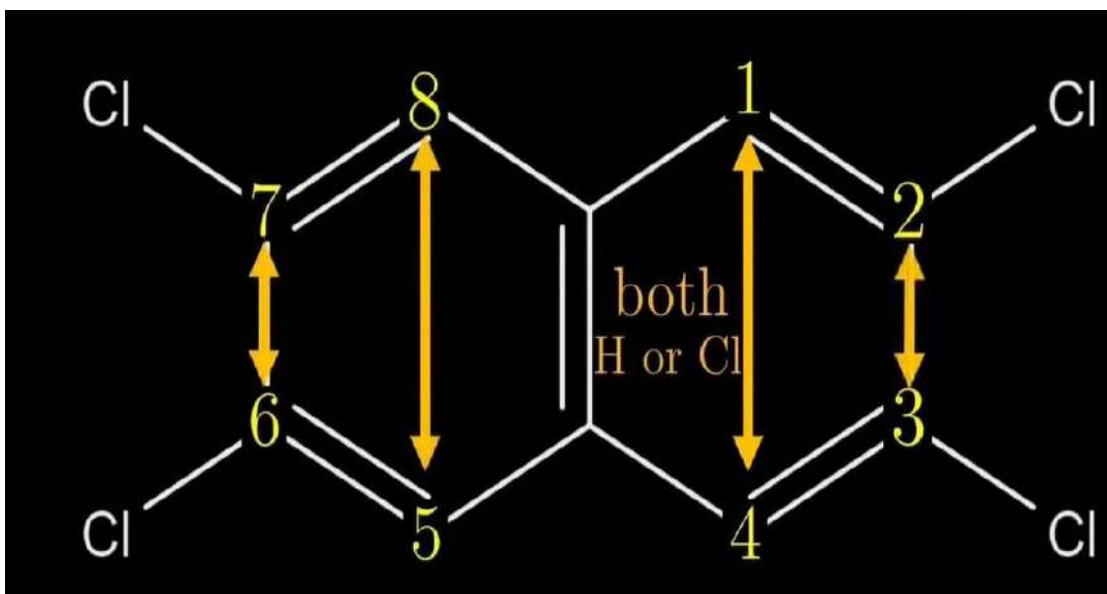


Fig:-Tetrachloronaphthalene

So, out of the four pairs of places for the Chlorine (Cl) substituent, we choose two.

So it's the fix size = 4C_2

Similarly, in the remaining two symmetries the fix size is 4C_2 .

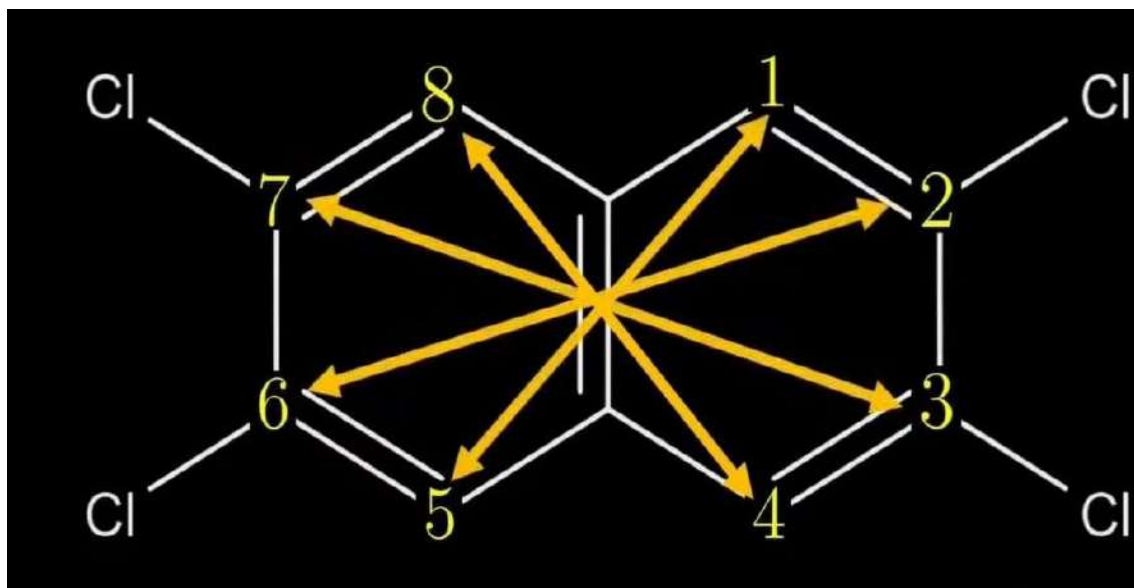


Fig:-Tetrachloronaphthalene

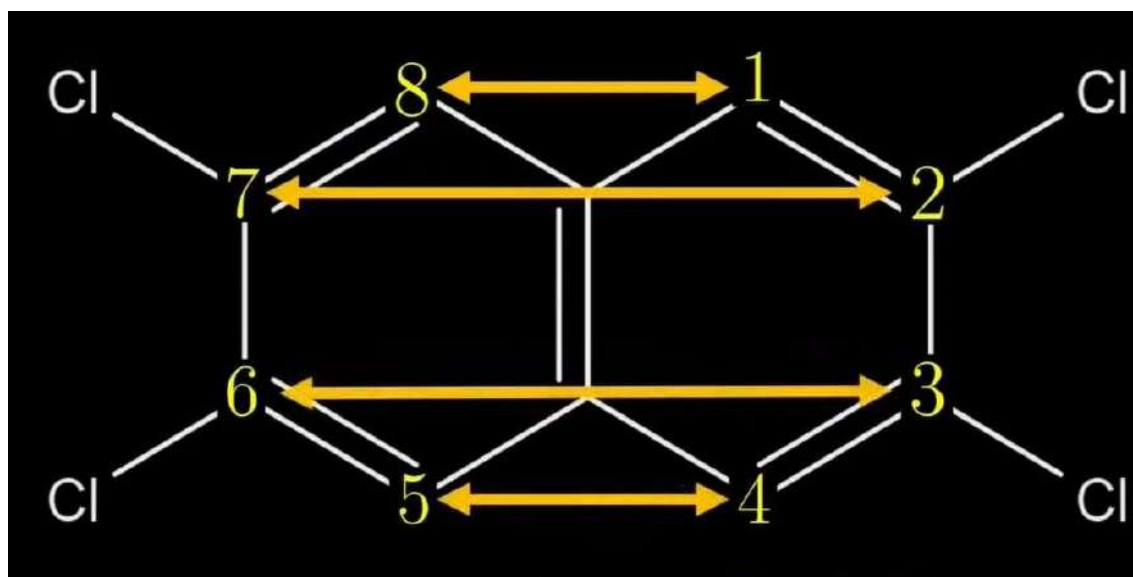


Fig:-Tetrachloronaphthalene

$$\text{Total fix size} = {}^8C_4 + 3 \cdot {}^4C_2 = 88$$

$$\text{By Burnside's Lemma \# of orbits} = 88/4 = 22$$

CONCLUSION:-

We have already seen that Burnside's Lemma has numerous and remarkable applications. One of the most extensively researched in graphical and chemical isomer enumeration, but there are plenty of other uses as well like-

- To investigate crystal structure and studying nuclear magnetic resonance and NMR space.
- Enumerating the number of Boolean function under various conditions.
- Counting finite automata and certain binary matrices.
- Study kinetic structures.

Thus if we this properties property in various fields then our studies will be more helpful and interesting for upcoming generation.

REFERENCE:-

- Jenny, J., Analysis an application of Burnside's lemma. 2018, 1-11.
- Huisinga, M., Polya's counting theory. 2012, 1-46.
- Goluguri, I., Christina, L., Applications of group actions. 2019, 1-10.

***RAMAKRISHNA MISSION VIVEKANANDA CENTENARY
COLLEGE***

- **Name: Souvik Pal**
- **Reg no: A01-1152-113-036-2019**
- **Roll: 2022151118**
- **College roll: 352**
- **Topic: Cayley's theorem by group homomorphism and
Group action**
- **Supervised by: Prof. Pravanjan Kumar Rana**

ACKNOWLEDGEMENT

We would like to express my special thanks of gratitude to our group theory teacher “Mr. Pravanjan Kumar Rana” for his able guidance and support in completing this project.

I would also like to extend my gratitude to principal “swami Kamalasthanada maharaj” for providing me with all facility that was required.

Date:

15-01-2022

Amit Kumar Ghosh (2022151113)

Sanjay Karmakar (2022151111)

Souvik Pal (2022151118)

■ **CONTENTS:**

- **Definition of group action**
- **Definition of group homomorphism**
- **Induced homomorphism**
- **Cayley's theorem**
- **Proof by Cayley's theorem**
(by group homomorphism method)
(by group action method)

TOPIC: CAYLEY'S THEOREM BY GROUP HOMOMORPHISM AND GROUP ACTION

Definition of Group Action:

Let G be a group and X be a set. Then G is said to act on X if there is a mapping $\phi: G \times X \rightarrow X$, with $\phi(a, x)$ written $a * x$ such that for all $a, b \in G, x \in X$

- $a * (b * x) = ab * x$
- $e * x = x$

The mapping ϕ is called **the action of G on X** , and X is said to be a G -set.

Definition of Group homomorphism:

Let $(G, *)$ and (G', \circ) be two groups and f be a function from G into G' . Then f is called a **group homomorphism** of G to G' if for all $a, b \in G$,

$$f(a * b) = f(a) \circ f(b)$$

Theorem:

Let G be a group and let X be a set.

- If X is a G -set, then the action of G on X induces a homomorphism $\phi: G \rightarrow S_X$.
- Any homomorphism $\phi: G \rightarrow S_X$ induces an action of G onto X .

Proof:

At first we define $\phi: G \rightarrow S_X$ by $(\phi(a))(x) = ax$, $a \in G, x \in X$

Now we have to prove $\phi(a) \in S_X$

Let $x_1, x_2 \in X$

Then,

$$(\phi(a))(x_1) = (\phi(a))(x_2)$$

$$\Rightarrow ax_1 = ax_2$$

$$\Rightarrow x_1 = x_2$$

$\therefore \phi(a)$ is one-one.

Now,

$$\begin{aligned} x_2 &= a(a^{-1}x_2) \\ &= (\phi(a))(a^{-1}x_2) \quad , a^{-1}x_2 \in X \end{aligned}$$

Thus, $\phi(a) \in S_X$

Now, let, $a, b \in G$

Then

$$\begin{aligned} \phi(ab)(x) &= (ab)(x) \\ &= a(bx) \\ &= a(\phi(b)(x)) \\ &= \phi(a)\phi(b)(x) \quad , \forall x \in X \end{aligned}$$

Here, $\phi(ab) = \phi(a)\phi(b)$

So, ϕ is a homomorphism.

Now we define,

$$a * x = \phi(a)(x)$$

That is $ax = (\phi(a))(x)$

Let, $a, b \in G$

Then

$$\begin{aligned}
(ab)(x) &= (\phi(ab))(x) \\
&= (\phi(a)\phi(b))(x) \\
&= \phi(a)(\phi(b)(x)) \\
&= \phi(a)(bx) \\
&= a(bx)
\end{aligned}$$

Also $ex = (\phi(e))(x) = e$ (where e is the identity element)

Hence X is a G -set.

Application: Cayley's Theorem:

Let G be a group. Then G is isomorphic to a subgroup of group S_G .

Proof by group action method:

Here we want to prove this theorem by the group action method.

G is a G -set.

Where G acts on G by group operation.

This left action induces a homomorphism $\phi: G \rightarrow S_G$

Where $(\phi(a))(x) = ax \quad a \in G, x \in G$

$$\begin{aligned}
\text{Ker}\phi &= \{a \in G : \phi(a) = \text{identity permutation on } G\} \\
&= \{a \in G : ax = x, \forall x \in G\} \\
&= \{e\}
\end{aligned}$$

Hence ϕ is a monomorphism.

Now by first isomorphism theorem $\frac{G}{\text{ker}\phi} \cong \text{subgroup of } S_G$

So, the theorem is proved.

Proof by group homomorphism method:

Here we want to prove this theorem by the homomorphism method.

Let G be a group.

For any $a \in G$ the mapping $f_a : G \rightarrow G$, given by $f_a(x) = ax$ for all $x \in G$ is a bijection, because,

$$\begin{aligned} ax &= ax' \\ \Rightarrow x &= x' \end{aligned}$$

And $y = f_a(a^{-1}y)$ for all $x, x', y \in G$

Considering the mapping, $\phi : G \rightarrow S_G$

Where $\phi(a) = f_a$ for all $a \in G$

Where S_G is a symmetric group on the set G

Now, for all $a, b, x \in G$,

$$\begin{aligned} f_{ab}(x) &= abx \\ &= f_a(bx) \\ &= f_a(f_b(x)) \\ &= (f_a f_b)(x) \end{aligned}$$

Hence $\phi(ab) = \phi(a)\phi(b)$

Therefore, ϕ is a homomorphism.

And $\text{Im } \phi$ is a subgroup of S_G

Moreover,

$$\begin{aligned} \phi(a) &= \phi(b) \\ \Rightarrow ax &= bx \quad \forall x \in G \\ \Rightarrow a &= b \end{aligned}$$

Hence ϕ is an injective homomorphism.

Therefore G is isomorphic to a subgroup of S_G

The above isomorphism is called the **left regular representation** of G .

Similarly, we have a right regular representation.

Reference:

To write this project, we take help of these following books,

- Abstract Algebra (Dummit, David, Foote)
- Contemporary abstract algebra (Joseph Gallian)
- Fundamentals of Abstract Algebra (Malik, Moderesen, Sen)

**RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE
RAHARA, KOLKATA:-700118**

Department of Mathematics

Semester: 5th

Core Course:-XII (Group Theory-II)

**Project Title:- BURNSIDE'S LEMMA AND IT'S
APPLICATION**

Submitted By:

Subrata Khanra (Examination Roll No:-2022151106,

Reg. No:- A01-1112-113-018-2019)

Souvik Dolai (Examination Roll No:-2022151116,

Reg. No:-A01-1122-113-033-2019)

Sayan Ghosh (Examination Roll No:-2022151127,

Reg. No:-A01-1112-113-049-2019)

Supervised By:

Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and our special gratitude to **Dr. Pravanjan Kumar Rana, Head of the department of mathematics of RKMVCC Rahara** , who gave us a golden opportunity to do this project and also provided support in completing my project work.

CONTENTS

<u>Sl. No</u>	<u>Title</u>	<u>Page No</u>
1	Abstract	1
2	Introduction	1
3	Discussion	2-4
4	Application of Burnside's Lemma	5-8
5	Conclusion	8
6	Reference	8

BURNSIDE'S LEMMA AND IT'S APPLICATION

ABSTRACT:-

Burnside's Lemma, also referred to as Orbit Counting Theorem, is a result of group theory that used to count distinct objects with respect to symmetry. It provides a formula to count the number of object, where two objects that are symmetry by rotation or reflection are not categorized as distinct.

The result of this Theorem has been extensively used, in particular to enumeration of chemical isomer compounds.

INTRODUCTION:-

Mathematics is the cradle of all creation be it a farmer or a engineer, a shopkeeper or a doctor, a scientist or a magician everyone needs mathematics in their day to day life.

In this project we show how we can solve non mathematical problems with the help of Burnside's Lemma. Now we apply this theorem to a chemistry molecule in enumeration of different chemical structure are called isomers.

DISCUSSION:-

As Burnside's Lemma is a result of group theory, we will first provide some basic definitions and notations involved in group theory that will be relevant in this paper.

Let we have a group G that acts on a set X . We illustrate the groups as the following dots inside the box.

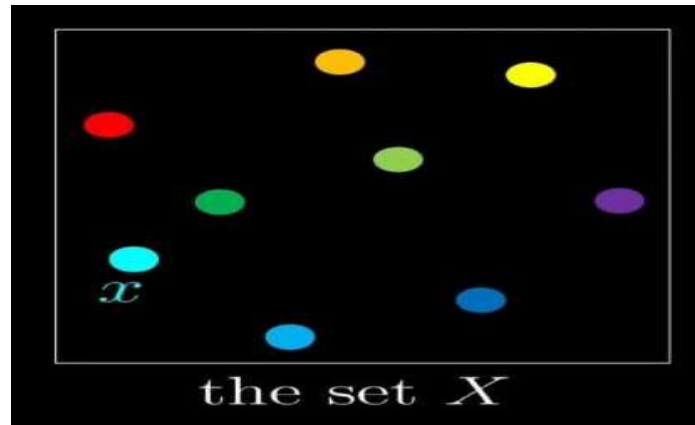


Fig:-1

Let we pick a x among the dots. Then we define its orbit where x can go under the action.

$$\text{Orbit}_G(X) = \{\text{where } x \text{ can go}\}.$$

So the elements in orbit of x are elements from the set X .

$$\text{Stab}_G(X) = \{\text{elements of } G \text{ that fixes } x\}$$

The Orbit-Stabilizer Theorem basically says that the product of the size of orbit and stabilizer of an element in X is the size of the whole group G .

We will prove Burnside's Lemma using the Orbit-Stabilizer Theorem, basically counts the number of orbits in X . We will do this using some diagram and some word as well.

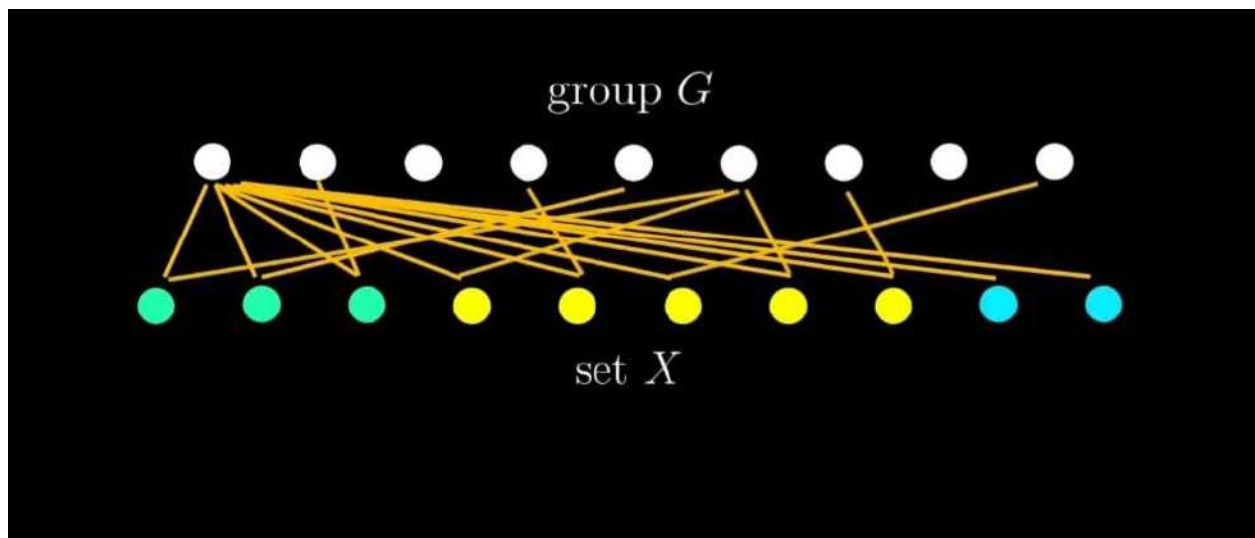


Fig:-2

In the upper picture we draw elements of G and X . Then we will draw lines from the elements of G to the elements of X . The condition of drawing the lines if $g \in G$ fixes $x \in X$ i.e. $g.x = x$ then we will draw line from g to x . The point in G marked as 1 is the identity in G .

Since identity element fixes every element in X , we have drawn lines to every element in X from the point 1.

Now we want to count the number of lines we have drawn here. From the picture we write the following table-

<u>Elements in G</u>	<u>No of lines from the elements</u>
1	10
2	1
3	0
4	1
5	1
6	3
7	1
8	0
9	1

Number in the right column of the table are the number of elements in X fixed by corresponding elements of G in left column. For example 4 fixes one elements in X .

We call the set of elements in X fixed by g in G as $\text{fix}(g)$. So the number in right columns are nothing but corresponding $|\text{fix}(g)|$. Therefore the sum $\sum_{g \in G} \text{fix}(g)$ is nothing but the number of total lines.

Now we will count again the number of lines but this time in a different way.

Let's see the lines from the lower row of figure 1 i.e. the elements of X . The collection of elements of X marked with second lying bracket are elements of same orbits. A line from $x \in X$ is drawn if g fixes x i.e. $g \in \sum_G \text{Stab}(x)$.

So the number of lines drawn from a point x in X is precisely the size of stabilizer of x that is $|\text{Stab}_G(X)|$.

Now by the Orbit-Stabilizer Theorem for any a in X

$$|\text{stab}_G(a)| = |G|/|\text{Orb}_G(a)|$$

Since order of orbit for each element in same orbit is same, we conclude that order of Stab of each element in same orbit is also same.

Therefore the total number of lines drawn from an orbit is give a number of lines drawn from one element X number of elements in the orbit, that is $|\text{Stab}_G(X)| * |\text{Orbit}_G(X)|$ that is nothing but $|G|$.

Therefore the total number of lines drawn from elements of X is the number of lines drawn from each orbit = (number of orbit) * $|G|$. Since the number of line cannot be different due to variations in counting, we have

$$(\text{Number of orbit}) * |G| = \sum_{g \in G} \text{fix}(g)$$

$$\text{So, Number of orbit} = 1/|G| * \sum_{g \in G} |\text{fix}(g)|$$

This is the awaited Burnside's Lemma.

APPLICATION OF BURNSIDE'S LEMMA

Burnside's Lemma has variety of application that has been adapted to many different fields of study. The most widely known application is within chemical isomer enumeration.

Chemical isomer enumeration:-

In chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecule in space. The molecules that have the same chemical formula but different chemical structures are called isomers, and we can use Burnside's Lemma to enumerate these type of isomers.

Let's look at an example,

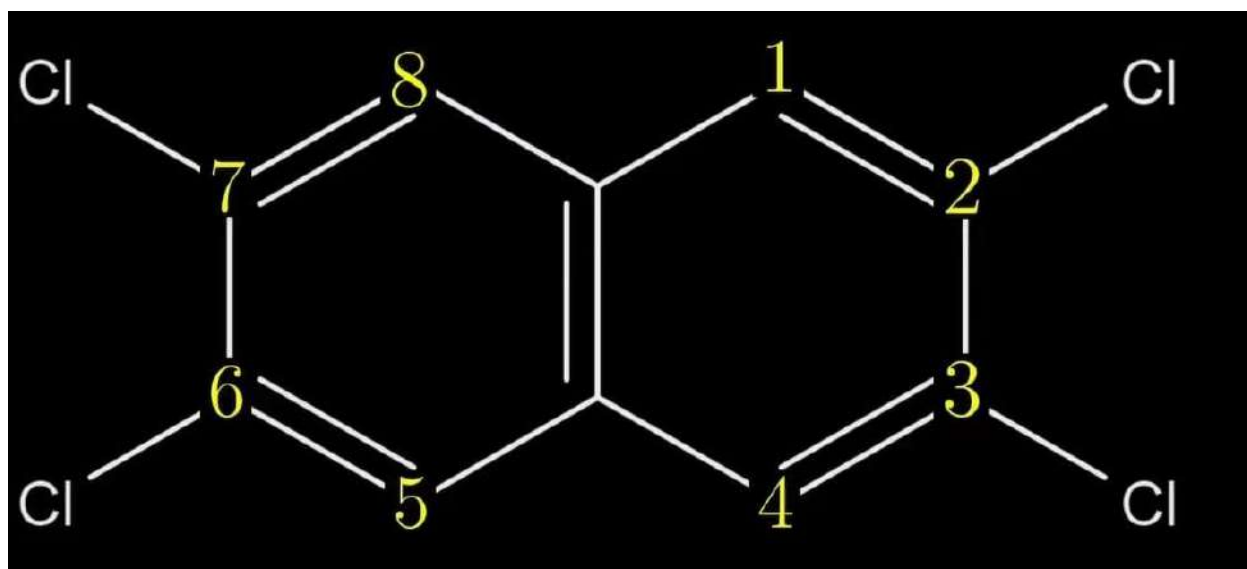


Fig:-Tetrachloronaphthalene

Now, our question is –

How much naphthalene with 4 chlorine (Cl) substituent?

We can use Burnside's Lemma to determine the required number. Here we consider four symmetries-

- ❖ Identity
- ❖ Horizontal reflection
- ❖ Vertical reflection
- ❖ 180° rotation

Burnside's Lemma: $\# \text{ Of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$

We can substitute the size of the group $|G|=4$

- First we consider the fix elements of the identity. By definition, identity fixes everything. Out of the total eight positions in naphthalene, we can choose only four different sites in the molecules where we can substitute one H by chlorine (Cl).
So its fix size = 8C_4
- Now we consider the fix size for the horizontal reflection. In this symmetry, 1 is swapped with 4, so the same thing. That is both must have the chlorine (Cl) or both not having the chlorine (Cl).

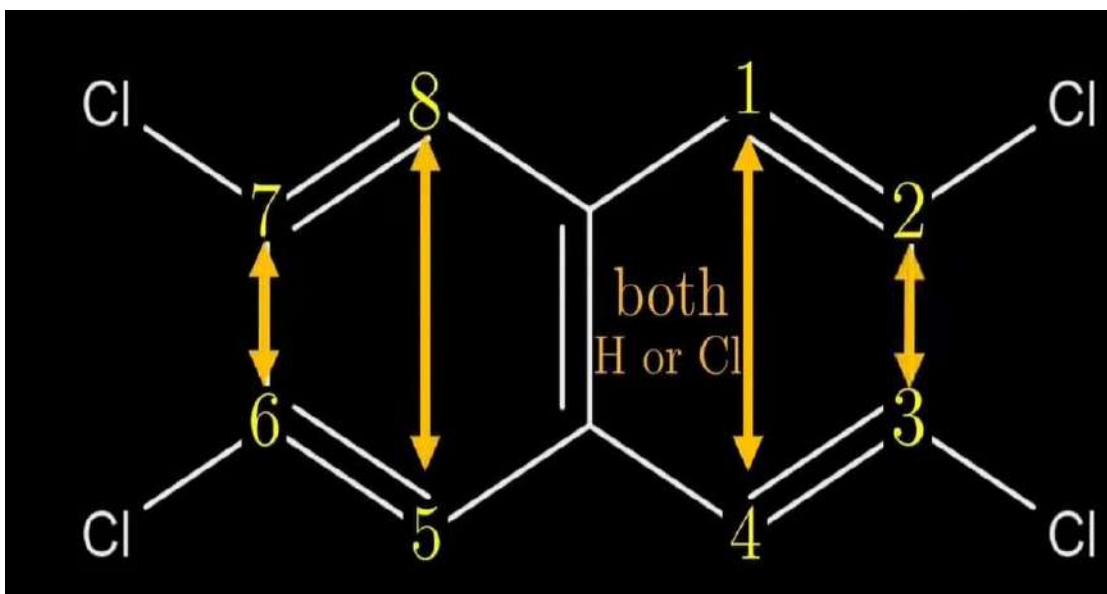


Fig:-Tetrachloronaphthalene

So, out of the four pairs of places for the Chlorine (Cl) substituent, we choose two.

So it's the fix size = 4C_2

Similarly, in the remaining two symmetries the fix size is 4C_2 .

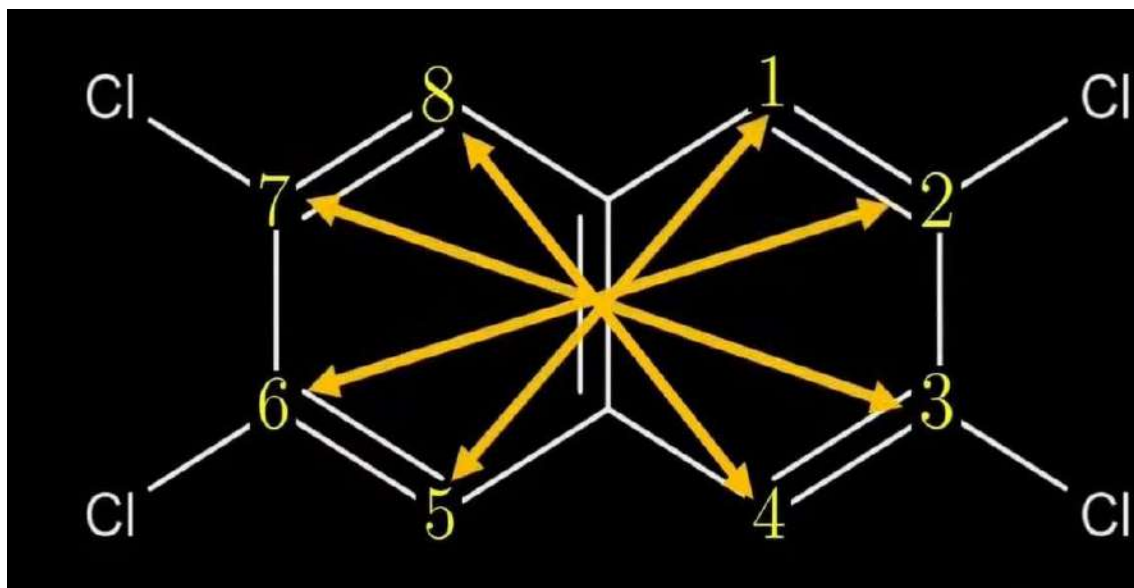


Fig:-Tetrachloronaphthalene

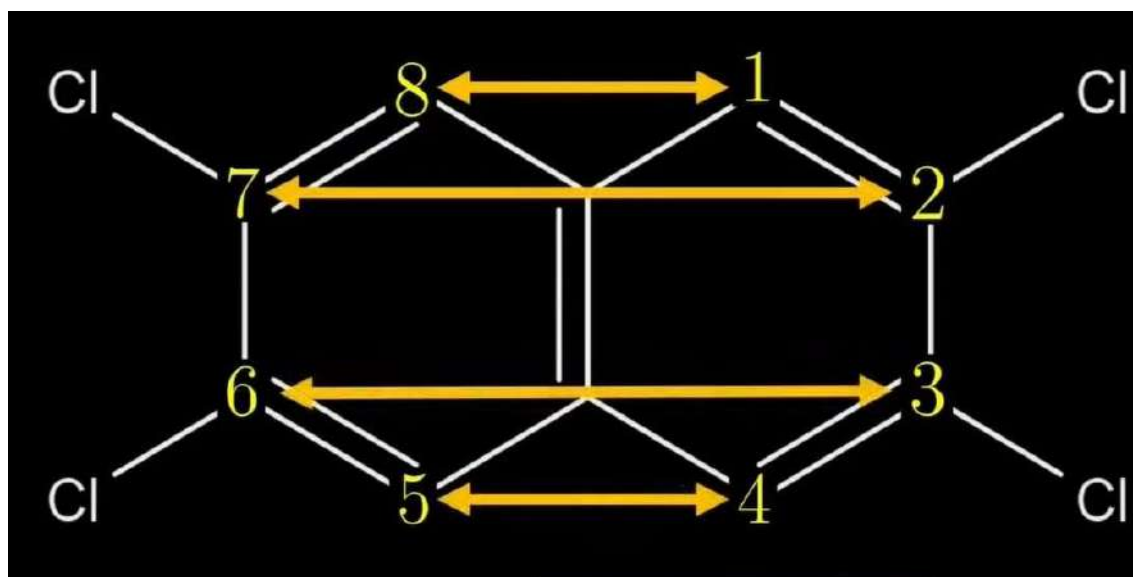


Fig:-Tetrachloronaphthalene

$$\text{Total fix size} = {}^8C_4 + 3 \cdot {}^4C_2 = 88$$

$$\text{By Burnside's Lemma \# of orbits} = 88/4 = 22$$

CONCLUSION:-

We have already seen that Burnside's Lemma has numerous and remarkable applications. One of the most extensively researched in graphical and chemical isomer enumeration, but there are plenty of other uses as well like-

- To investigate crystal structure and studying nuclear magnetic resonance and NMR space.
- Enumerating the number of Boolean function under various conditions.
- Counting finite automata and certain binary matrices.
- Study kinetic structures.

Thus if we this properties property in various fields then our studies will be more helpful and interesting for upcoming generation.

REFERENCE:-

- Jenny, J., Analysis an application of Burnside's lemma.
2018, 1-11.
- Huisinga, M., Polya's counting theory.
2012, 1-46.
- Goluguri, I., Christina, L., Applications of group actions.
2019, 1-10.

**RAMAKRISHNA MISSION VIVEKANANDA
CENTENARY COLLEGE
RAHARA, KOLKATA:-700118**

Department of Mathematics

Semester: 5th

Core Course:-XII (Group Theory-II)

**Project Title:- BURNSIDE'S LEMMA AND IT'S
APPLICATION**

Submitted By:

Subrata Khanra (Examination Roll No:-2022151106,

Reg. No:- A01-1112-113-018-2019)

Souvik Dolai (Examination Roll No:-2022151116,

Reg. No:-A01-1122-113-033-2019)

Sayan Ghosh (Examination Roll No:-2022151127,

Reg. No:-A01-1112-113-049-2019)

Supervised By:

Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and our special gratitude to **Dr. Pravanjan Kumar Rana, Head of the department of mathematics of RKMVCC Rahara** , who gave us a golden opportunity to do this project and also provided support in completing my project work.

CONTENTS

<u>Sl. No</u>	<u>Title</u>	<u>Page No</u>
1	Abstract	1
2	Introduction	1
3	Discussion	2-4
4	Application of Burnside's Lemma	5-8
5	Conclusion	8
6	Reference	8

BURNSIDE'S LEMMA AND IT'S APPLICATION

ABSTRACT:-

Burnside's Lemma, also referred to as Orbit Counting Theorem, is a result of group theory that used to count distinct objects with respect to symmetry. It provides a formula to count the number of object, where two objects that are symmetry by rotation or reflection are not categorized as distinct.

The result of this Theorem has been extensively used, in particular to enumeration of chemical isomer compounds.

INTRODUCTION:-

Mathematics is the cradle of all creation be it a farmer or a engineer, a shopkeeper or a doctor, a scientist or a magician everyone needs mathematics in their day to day life.

In this project we show how we can solve non mathematical problems with the help of Burnside's Lemma. Now we apply this theorem to a chemistry molecule in enumeration of different chemical structure are called isomers.

DISCUSSION:-

As Burnside's Lemma is a result of group theory, we will first provide some basic definitions and notations involved in group theory that will be relevant in this paper.

Let we have a group G that acts on a set X . We illustrate the groups as the following dots inside the box.

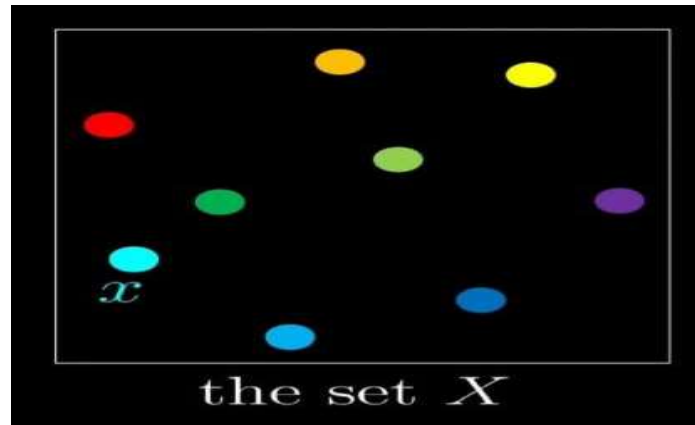


Fig:-1

Let we pick a x among the dots. Then we define its orbit where x can go under the action.

$$\text{Orbit}_G(X) = \{\text{where } x \text{ can go}\}.$$

So the elements in orbit of x are elements from the set X .

$$\text{Stab}_G(X) = \{\text{elements of } G \text{ that fixes } x\}$$

The Orbit-Stabilizer Theorem basically says that the product of the size of orbit and stabilizer of an element in X is the size of the whole group G .

We will prove Burnside's Lemma using the Orbit-Stabilizer Theorem, basically counts the number of orbits in X . We will do this using some diagram and some word as well.

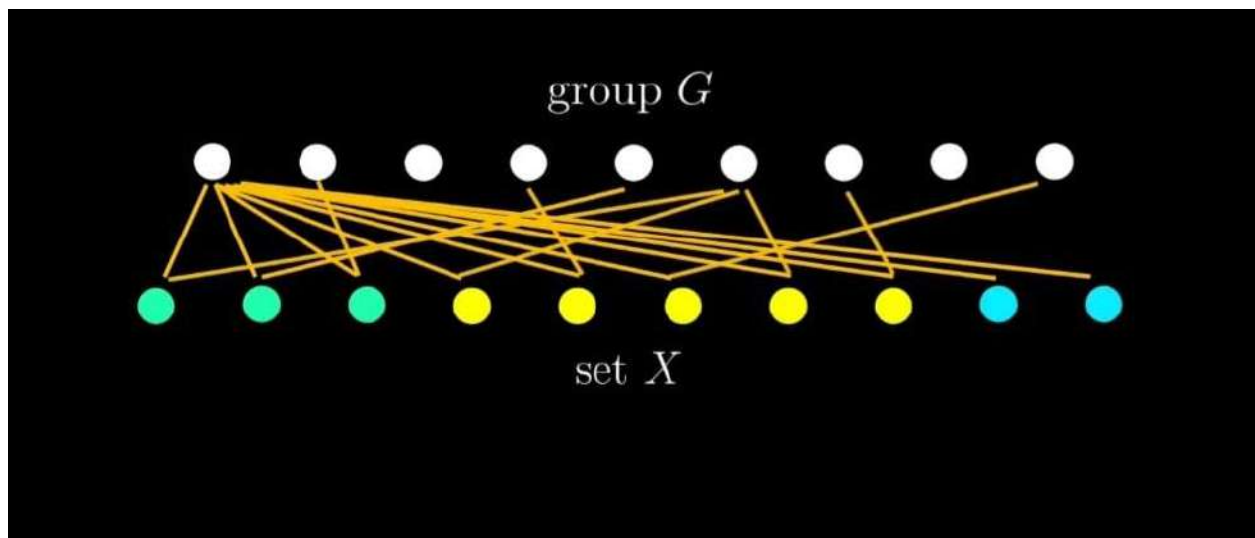


Fig:-2

In the upper picture we draw elements of G and X . Then we will draw lines from the elements of G to the elements of X . The condition of drawing the lines if $g \in G$ fixes $x \in X$ i.e. $g.x = x$ then we will draw line from g to x . The point in G marked as 1 is the identity in G .

Since identity element fixes every element in X , we have drawn lines to every element in X from the point 1.

Now we want to count the number of lines we have drawn here. From the picture we write the following table-

<u>Elements in G</u>	<u>No of lines from the elements</u>
1	10
2	1
3	0
4	1
5	1
6	3
7	1
8	0
9	1

Number in the right column of the table are the number of elements in X fixed by corresponding elements of G in left column. For example 4 fixes one elements in X .

We call the set of elements in X fixed by g in G as $\text{fix}(g)$. So the number in right columns are nothing but corresponding $|\text{fix}(g)|$. Therefore the sum $\sum_{g \in G} \text{fix}(g)$ is nothing but the number of total lines.

Now we will count again the number of lines but this time in a different way.

Let's see the lines from the lower row of figure 1 i.e. the elements of X . The collection of elements of X marked with second lying bracket are elements of same orbits. A line from $x \in X$ is drawn if g fixes x i.e. $g \in \sum_G \text{Stab}(x)$.

So the number of lines drawn from a point x in X is precisely the size of stabilizer of x that is $|\text{Stab}_G(X)|$.

Now by the Orbit-Stabilizer Theorem for any a in X

$$|\text{stab}_G(a)| = |G|/|\text{Orb}_G(a)|$$

Since order of orbit for each element in same orbit is same, we conclude that order of Stab of each element in same orbit is also same.

Therefore the total number of lines drawn from an orbit is give a number of lines drawn from one element X number of elements in the orbit, that is $|\text{Stab}_G(X)| * |\text{Orbit}_G(X)|$ that is nothing but $|G|$.

Therefore the total number of lines drawn from elements of X is the number of lines drawn from each orbit = (number of orbit) * $|G|$. Since the number of line cannot be different due to variations in counting, we have

$$(\text{Number of orbit}) * |G| = \sum_{g \in G} \text{fix}(g)$$

$$\text{So, Number of orbit} = 1/|G| * \sum_{g \in G} |\text{fix}(g)|$$

This is the awaited Burnside's Lemma.

APPLICATION OF BURNSIDE'S LEMMA

Burnside's Lemma has variety of application that has been adapted to many different fields of study. The most widely known application is within chemical isomer enumeration.

Chemical isomer enumeration:-

In chemistry, a chemical formula can represent more than one molecule due to varying arrangements of the molecule in space. The molecules that have the same chemical formula but different chemical structures are called isomers, and we can use Burnside's Lemma to enumerate these type of isomers.

Let's look at an example,

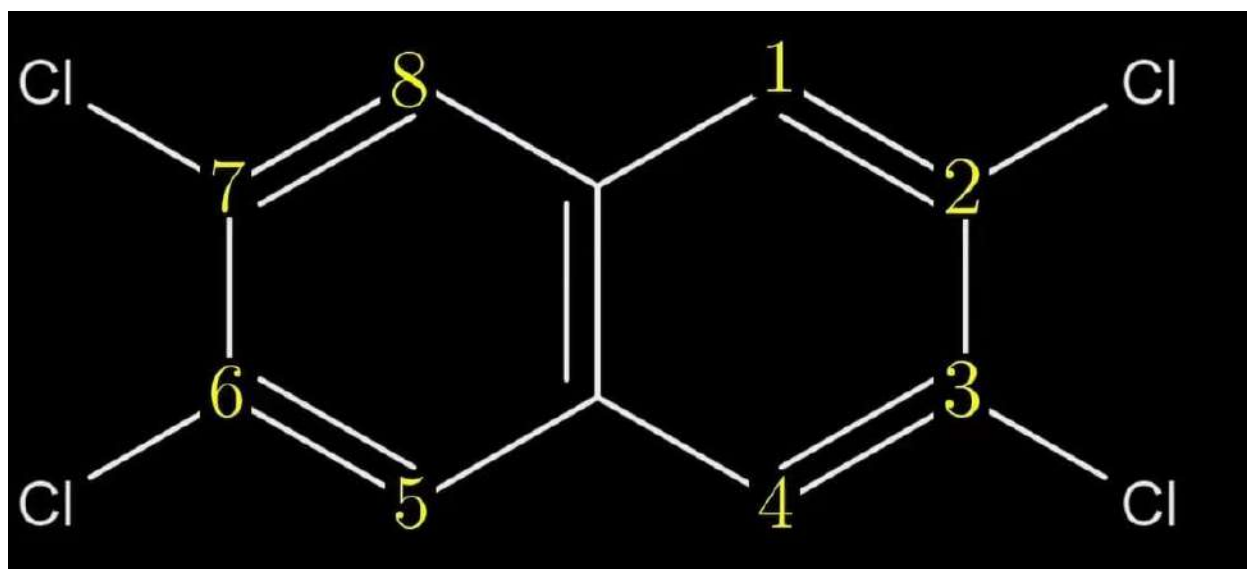


Fig:-Tetrachloronaphthalene

Now, our question is –

How much naphthalene with 4 chlorine (Cl) substituent?

We can use Burnside's Lemma to determine the required number. Here we consider four symmetries-

- ❖ Identity
- ❖ Horizontal reflection
- ❖ Vertical reflection
- ❖ 180° rotation

Burnside's Lemma: $\# \text{ Of orbits} = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$

We can substitute the size of the group $|G|=4$

- First we consider the fix elements of the identity. By definition, identity fixes everything. Out of the total eight positions in naphthalene, we can choose only four different sites in the molecules where we can substitute one H by chlorine (Cl).
So its fix size = 8C_4
- Now we consider the fix size for the horizontal reflection. In this symmetry, 1 is swapped with 4, so the same thing. That is both must have the chlorine (Cl) or both not having the chlorine (Cl).

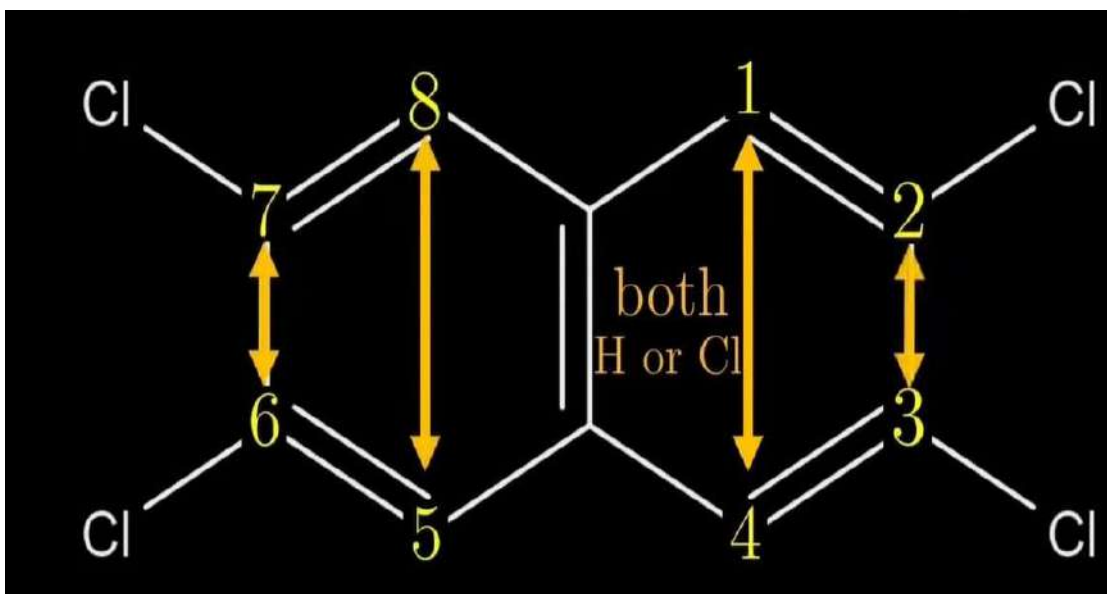


Fig:-Tetrachloronaphthalene

So, out of the four pairs of places for the Chlorine (Cl) substituent, we choose two.

So it's the fix size = 4C_2

Similarly, in the remaining two symmetries the fix size is 4C_2 .

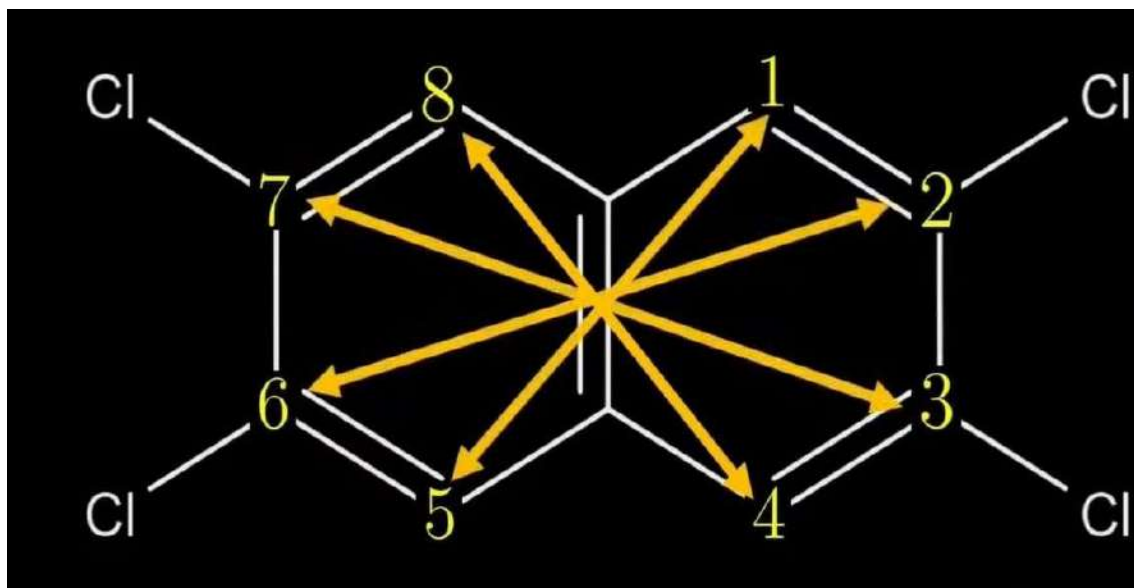


Fig:-Tetrachloronaphthalene

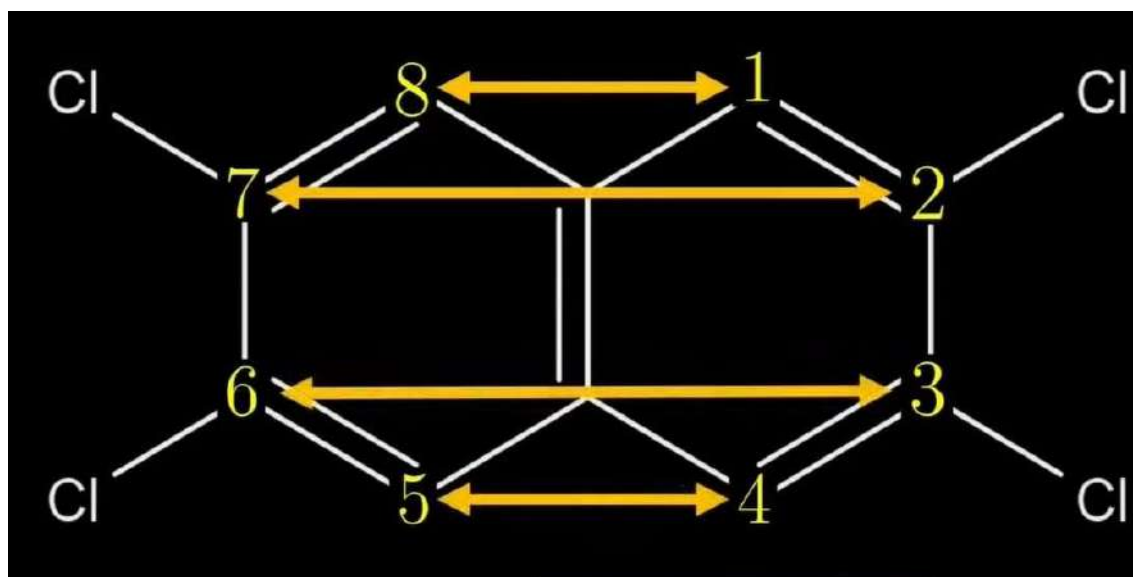


Fig:-Tetrachloronaphthalene

$$\text{Total fix size} = {}^8C_4 + 3 \cdot {}^4C_2 = 88$$

$$\text{By Burnside's Lemma \# of orbits} = 88/4 = 22$$

CONCLUSION:-

We have already seen that Burnside's Lemma has numerous and remarkable applications. One of the most extensively researched in graphical and chemical isomer enumeration, but there are plenty of other uses as well like-

- To investigate crystal structure and studying nuclear magnetic resonance and NMR space.
- Enumerating the number of Boolean function under various conditions.
- Counting finite automata and certain binary matrices.
- Study kinetic structures.

Thus if we this properties property in various fields then our studies will be more helpful and interesting for upcoming generation.

REFERENCE:-

- Jenny, J., Analysis an application of Burnside's lemma. 2018, 1-11.
- Huisinga, M., Polya's counting theory. 2012, 1-46.
- Goluguri, I., Christina, L., Applications of group actions. 2019, 1-10.

Satyabrata Pradhan

Registration No : A01-1112-113-027-2019

Roll no : 340

Semester : 5

Paper : CC-12

**Topic : The Framework of Music Theory as
Represented with Groups**

Acknowledgement

I would like to express my special thanks of gratitude to our beloved **Pravanjan Kumar Rana Sir** who gave me the opportunity to do this wonderful project on the topic **The Framework of Music Theory as Represented with Groups**, which also helped me in doing a lot of research and I come to know about so many new things.

Secondly I would like to thank my friends **Pranay Mandal** and **Shubhajit Bhowmick** who helped me a lot in finishing this project within the limited. It helped me increase my knowledge and skills.

The Framework of Music Theory as Represented with Groups

Contents

- 1 Introduction
- 2 Basic Group Theory
 - 2.1 What is a group ?
 - 2.2 Permutations
 - 2.3 Morphisms
 - 2.3.1 Homomorphisms
 - 2.3.2 Isomorphisms
 - 2.3.3 Automorphisms
 - 2.4 Products
 - 2.4.1 Direct Products
 - 2.4.2 Semidirect Products
 - 2.4.3 Wreath Products
- 3 Music Theory
 - 3.1 Basic concepts of atonal music theory
 - 3.1.1 T_n , the Transpositions
 - 3.1.2 $T_n I$, the Inversions
- 4 Group Theory as a Structure for Atonal Music Theory
- 5 A Flaw in Atonal Music Theory

6 Uniform Triadic Transformations

6.1 Introduction to Triadic Transformations

6.2 V , the Uniform Triadic Transformations

6.2.1 Multiplication on V

6.2.2 Inversion on V

6.2.3 Isomorphism to $Z_{12} \wr Z_2$

6.2.4 Even and Odd UTTs

6.3 R , the Riemannian UTTs

6.4 K , the Subgroups of V

7 Musical Application

8 Conclusion

References

1. Introduction

In 2002, a music theorist by the name of Julian Hook published a paper in the Journal of Music Theory titled, “Uniform Triadic Transformations.” In this paper, Hook generalized some existing music theoretical concepts and greatly improved their notation. Hook’s UTTs formed a group with interesting algebraic properties.

This paper will first give the reader a review of all necessary group theory to understand the discussion of Hook’s UTTs. Then it will review music theory (atonal theory in particular) and its evolution to the UTTs. Finally, it will discuss the UTTs themselves and conclude with some musical applications.

2 . Basic Group Theory

Group theory is a branch of mathematics that studies groups. This algebraic structure forms the basis for abstract algebra, which studies other structures such as rings, fields, modules, vector spaces and algebras. These can all be classified as groups with addition operations and axioms.

This section provides a quick and basic review of group theory, which will serve as the basis for discussions in the group theoretical structure as applied to music theory.

2.1 . What is a group?

A group is a set such that any two elements x and y can be combined via “multiplication” to form a unique product xy that also lies in the set. This multiplication is defined for every group and does not necessarily refer to the traditional meaning of “multiplication.” We now state the formal definition of a group:

Definition 2.1. A group is a set G together with a multiplication on G which satisfies three axioms:

- (a) The multiplication is associative, that is to say $(xy)z = x(yz)$ for any three (not necessarily distinct) elements in G .
- (b) There is an element $e \in G$, called an identity element, such that $xe = e = ex, \forall x \in G$
- (c) Each element $x \in G$ has an inverse x^{-1} which belongs to the set G and satisfies $x^{-1}x = e = xx^{-1}$

Theorem 2.2. Every group G satisfies the following properties:

- (a) The identity element e of G is unique
- (b) $\forall x \in G$, the inverse x^{-1} is unique

Note how commutativity of the multiplication is not required within a group. Therefore, we define an abelian group as follows:

Definition 2.3. A group G is abelian if its multiplication is commutative. That is, $xy = yx$ for any two elements in G .

To better illustrate the concept of a group, we now give some examples. Example 2.4. The reals excluding 0, $\mathbb{R} \setminus \{0\}$ under multiplication:

- The group is closed under multiplication: $\forall x, y \in \mathbb{R}, x \cdot y \in \mathbb{R}$
- The multiplication is associative: $\forall x, y, z \in \mathbb{R}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- The identity is 1: $\forall x \in \mathbb{R}, 1 \cdot x = x \cdot 1$
- The inverse of x is $\frac{1}{x}$: $\frac{1}{x} \cdot x = 1 = x \cdot \frac{1}{x}$

This group is abelian since $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$. Note how we must exclude 0 for this to be a group since there exists no inverse for 0. That is, there does not exist some $x \in \mathbb{R}$ such that $x \cdot 0 = 1$

Example 2.4. The integers $\mathbb{Z} \pmod{12}$, which we will denote as \mathbb{Z}_{12} , under addition $\pmod{12}$. (Note: in abstract algebra, $\mathbb{Z} \pmod{12}$ is generally notated as $\mathbb{Z}/(12)$ and \mathbb{Z}_{12} refers to another algebraic structure. However, in music theory, only $\mathbb{Z} \pmod{12}$ is of significance and we will use this more concise notation.)

- The group is closed under addition $\pmod{12}$: for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y \in \mathbb{Z}_{12}$.
- Addition $\pmod{12}$ is associative.
- The identity is 0.
- The inverse of x is $12-x$.

This group is also abelian since for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y = y +_{12} x$.

Example 2.6. The dihedral groups represent the symmetries of a regular polygon that map it onto itself. Consider the regular hexagon. Let r denote the rotation of through $\pi/3$ about the axis of symmetry perpendicular to the hexagon (rotating), let s denote the rotation through π about an axis of symmetry that lies in the plane of the plate (flipping), and let e denote the identity (leaving the hexagon unchanged). Then the dihedral group D_6 consists of the following 12 elements.

It may seem that the group is not closed under multiplication since the element sr is missing from the group. However, a rotation r takes the hexagon. A subsequent flip s takes the hexagon. Thus, rs is equivalent to r^5s . The reader can check that the whole group is indeed closed under multiplication. In general,

$$sr^n = r^{6-n}s, \forall n \in \mathbb{Z}_6$$

for the D_6 dihedral group.

Definition 2.7. The order of a group is the number of elements in the group.

Definition 2.8. The order of some element x of a group G is the smallest positive integer n such that $x^n = e$.

Definition 2.9. A subgroup of a group G is a subset of G which itself forms a group under the multiplication of G

Definition 2.10. A group G is cyclic if there exists an $x \in G$ such that for all $y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$. We call x a generator of G .

Definition 2.11. A permutation of an arbitrary set X is a bijection from X to itself.

Permutations can be denoted in multiple ways. Consider r from the D_6 dihedral group. We can represent it as a permutation of integers like so: (054321) , where each integer is sent to the one following it, and the final one is sent to the first. Likewise, we can write sr as $(01)(25)(34)$.

Definition 2.12. A permutation of the form $(a_1 a_2 \dots a_k)$ is called a cyclic permutation. A cyclic permutation of length k is called a k -cycle.

Definition 2.13. A transposition is 2-cycle. Any k -cycle $(a_1 a_2 \dots a_k)$ can be written as a product of transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$$

Note that transpositions may be written as many different products. This product is not unique, but is meant to show the existence of a product consisting only of transpositions.

Definition 2.14. An even permutation is a permutation that can be written as an even number of transpositions. The others are called odd permutations.

It may bother the reader that the a permutation in the form of a product of transpositions is not unique. Perhaps a permutation could be written as both an even number of transpositions and an odd number. However, the following theorem shows that the definition is well defined.

Theorem 2.15. Although any permutation can be written as a product of transpositions in infinitely many different ways, the number of transpositions which occur is always even or always odd.

Theorem 2.16. Consider the set X of n elements. The set of all permutations of X forms a group S_n called the symmetric group of degree n . Multiplication on this group is defined by composition of functions.

2.3 Morphisms

2.3.1 Homomorphisms

Definition 2.17. Let G and G' be groups. A homomorphism is a function $\phi : G \rightarrow G'$ that preserves the multiplication of G . Therefore, $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$

Example 2.18. Let ϕ be a function from D_{12} to Z_2 defined by $\psi(r^n) = 0$ and $\psi(r^n s) = 1$. Consider two elements x and y in D_{12} . We have four cases:

$$\bullet x = r^m, y = r^n;$$

$$\psi(xy) = \psi(r^m r^n) = \psi(r^{m+n}) = 0 = 0 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n;$$

$$\psi(xy) = \psi(r^m s r^n) = \psi(r^{m-n} s) = 1 = 1 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m, y = r^n s;$$

$$\psi(xy) = \psi(r^m r^n s) = \psi(r^{m+n} s) = 1 = 0 + 1 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n s;$$

$$\psi(xy) = \psi(r^m s r^n s) = \psi(r^{m-n} ss) = \psi(r^{m-n}) = 0 = 1 + 1 = \psi(x)\psi(y)$$

Hence, ϕ satisfies the properties of a homomorphism.

2.3.2 Isomorphisms

Definition 2.19. An isomorphism is a bijective homomorphism.

Example 2.20. \mathbb{Z}_{12} is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$. Consider the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$(0,0) \quad (0,1) \quad (0,2) \quad (0,3)$$

$$(1,0) \quad (1,1) \quad (1,2) \quad (1,3)$$

$$(2,0) \quad (2,1) \quad (2,2) \quad (2,3)$$

Send each element (x, y) to $4x + y$ and you have \mathbb{Z}_{12}

2.3.3 Automorphisms

Definition 2.21. An automorphism of a group G is an isomorphism from G to G . The set of all automorphisms forms a group under composition of functions, which is called the automorphism group of G and written $\text{Aut}(G)$.

Automorphisms fix the identity and send generators to generators.

Example 2.22. Consider the automorphisms of \mathbb{Z}_4 . There are only two generators in this group: 1 and 3. Therefore, there are only two elements in $\text{Aut}(\mathbb{Z}_4)$: the trivial one, and the one that flips 1 and 3.

2.4 Products

2.4.1 Direct Products

Theorem 2.23. The set $G \times H$ of two groups G and H is a group that consists of the elements (g, h) where $g \in G$ and $h \in H$. Given two elements (g, h) and (g', h') of $G \times H$, multiplication on this group is defined by

$$(g, h)(g', h') = (gg', hh')$$

where the first term, gg' , inherits the multiplication of G , and the second, hh' , inherits the multiplication of H . We call this group the direct product $G \times H$ of G and H .

Proof. Associativity follows from the associativity in both G and H . The identity is (e, e) and the (g^{-1}, h^{-1}) is the inverse of (g, h) .

Example 2.24. Consider $\mathbb{Z}_4 \times \mathbb{Z}_2$. This group has 8 elements: $(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)$.

Multiplication is defined by

$$(x, y) + (x', y') = (x + 4x', y + 2y')$$

2.4.2. Semidirect Products

Theorem 2.25. Suppose we have the groups G, H and the homomorphism $\phi : G \rightarrow \text{Aut}(H)$. Then the “twisted” direct product forms a new group. Its elements are of the form (g, h) with $g \in G$ and $h \in H$ and multiplication is defined by

$$(g, h)(g', h') = (g \cdot \phi(h)(g'), h \cdot h').$$

We call this group the semidirect product of G and H .

Example 2.26. Consider the semidirect product $\mathbb{Z}_4 * \mathbb{Z}_2$. The elements in this group are the same as those in $\mathbb{Z}_4 \times \mathbb{Z}_2$ as listed in Example 2.24.

We need to define ϕ . There are only two automorphisms of \mathbb{Z}_4 as shown in Example 2.22. Let the trivial automorphism be denoted with e and the other with σ . Then, since $\phi : \mathbb{Z}_2 \rightarrow \text{Aut}(H)$, we have $\phi(0) = e$ and $\phi(1) = \sigma$.

Now we can perform multiplication on the group. Consider multiplying the elements $(0, 0)$ and $(1, 0)$. Since $\phi(0) = e$ this multiplication is just like that of the direct product:

$$(0, 0)(1, 0) = (0 + \phi(0)1, 0 + 0) = (0 + e(1), 0 + 0)(1, 0)$$

Now consider the elements $(1, 0)$ and $(0, 1)$.

$$(0, 1)(1, 0) = (0 + \phi(1)(1), 1 + 0) = (0 + \sigma(1), 1 + 0) = (3, 1)$$

2.4.3. Wreath Products

The generalized form of a wreath product $G \wr H$ is too complicated for the scope of this paper. Therefore, we will only consider the special case taking a wreath product with \mathbb{Z}_2 .

Consider the group G . Then $G \wr \mathbb{Z}_2$ is isomorphic to $(G \times G) * \mathbb{Z}_2$. We will discuss this semidirect product in the dihedral notation as in Example 2.27. Thus, let the elements of $G \times G$ be denoted by $r_1^m r_2^n$.

The automorphism for a wreath product must permute the parts of an element in $G \times G$. Since we only have two elements, r_1^m and r_2^n , the only non-trivial automorphism is to switch them. That is $\delta(r_1^m r_2^n) = r_2^n r_1^m$. Thus,

$$r_1^m r_2^n s = s \delta(r_1^m r_2^n) = s r_2^n r_1^m$$

3. Music Theory

Music theory is a tool and framework with which we explain our listening experience. However, both the tool and the term “listening experience” are loosely defined. They are dependent on the music.

During the mid-15th century, composers began constructing their pieces around a particular pitch, called the tonic. This pitch was quickly established at the start of the piece and all other pitches were heard relative to it. Intervals and chords were labeled as consonant or dissonant. A feeling of tension occurred in various ways, such as when resolution was delayed, or when the music leapt to

distant keys (more than two accidentals removed from the tonic). Resolution to the tonic was crucial to ending the piece. After over two centuries of tonal music, listeners have begun to expect music to resolve in particular ways.

Along with the development of tonal music was the development of tonal theory. Its structure and notation allowed theorists to describe the listener's expectation. Thus, it provided an explanation for our reaction to particular harmonies. It explained our feeling of surprise at a particular chord and our feeling of finality at the end of a piece.

Around the turn of the 19th century, composers pushed the boundaries of tonal music. They began using dissonant chords with unprecedented freedom and resolved them in new ways. Eventually, their pieces no longer fit the framework of tonal music. Tonal theory no longer provided an adequate explanation for our listening experience. Thus, a new framework was constructed called atonal music theory.

Discussions in music require a certain vocabulary. The following terms are defined in the appendix:

- interval
- half step (semitone) & whole step (whole tone), flat, sharp, natural & accidental
- enharmonic equivalence
- major, minor, mode
- parallel & relative
- scale degree
- triad

3.1. Basic concepts of atonal music theory

Atonal music is based on sequences of pitches and intervals. No particular pitch is considered more important than the others and resolution of dissonance is unimportant. It assumes octave and enharmonic equivalence.

Definition 3.1. Pitches that are separated by an integer multiple of an octave, or are enharmonically equivalent belong to the same pitch class.

Definition 3.2. Consider the pitches a and b . The ordered pitch-class interval from a to b is $a-b \pmod{12}$.

Definition 3.3. A pitch-class set is an unordered set of pitch-classes, denoted as a string of integers enclosed in brackets. Within a pitch-class set, we do not have information about the register, rhythm or order of the pitches.

Example 3.4. The C major triad consists of the notes C, E and G. This can be represented as the pitch-class set [047], since $C = 0$, $E = 4$ and $G = 7$.

In atonal music, operations are performed on pitch-class sets, creating new pitch-class sets that are spread throughout the music. Thus, the music sounds random and yet structured at the same time. We will discuss two types of operations in this paper: the transpositions and the inversions.

3.1.1 T_n , the Transpositions

Definition 3.5. The transposition T_n moves a pitch-class or pitch-class set up by $n \pmod{12}$. (Note: moving down by n is equivalent to moving up by $12-n$.)

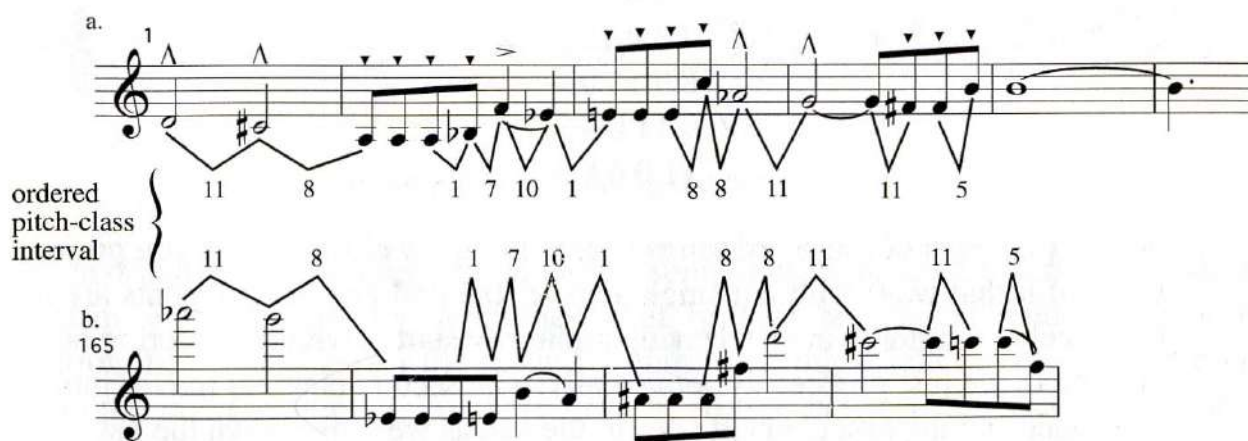


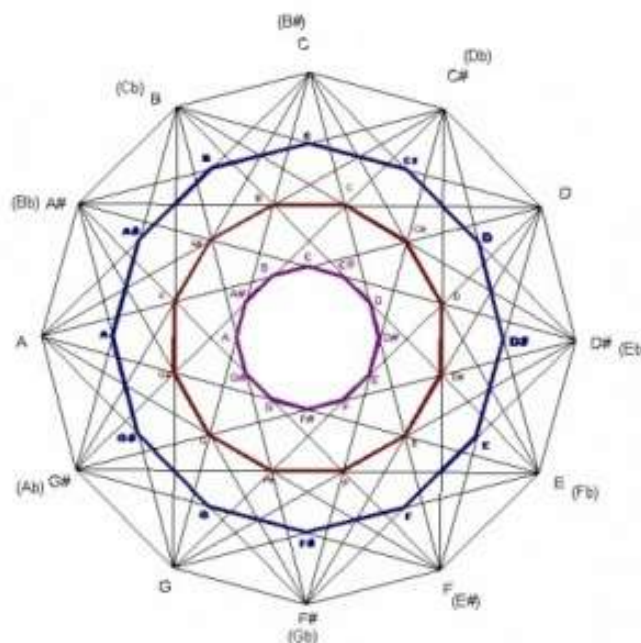
Figure 1: Two lines of pitch classes related by T6 (Schoenberg, String Quartet No. 4).

3.1.2 TnI, the Inversions

Definition 3.6. Consider the pitch a . Inversion $T_n I$ inverts the pitch about $C(0)$ and then transposes it by n . That is, $T_n I(a) = -a + n(\text{mod } 12)$.

4. Group Theory as a Structure for Atonal Music Theory

The numbering of the pitch classes reveals their isomorphism to \mathbb{Z}_{12} . More interestingly, the group of transpositions and inversions, denoted $T_n/T_n I$ is isomorphic to the dihedral group D_{12} .



Sehr langsam $\text{♩} = \text{ca. } 40$

Fl. 1 5

Ob.

Cl. 3 *pp*

Trp. 1 *pp* Immer mit Dmpf. 2 mit Dmpf. *p*

Vln. mit Dmpf. *pp*

Vla. 4 *p* *pp*

Piano *pp* *p* *pp*

1 2 3 4

Figure 3: Transpositionally equivalent pitch-class sets (Webern, Concerto for Nine Instruments, Op. 24).

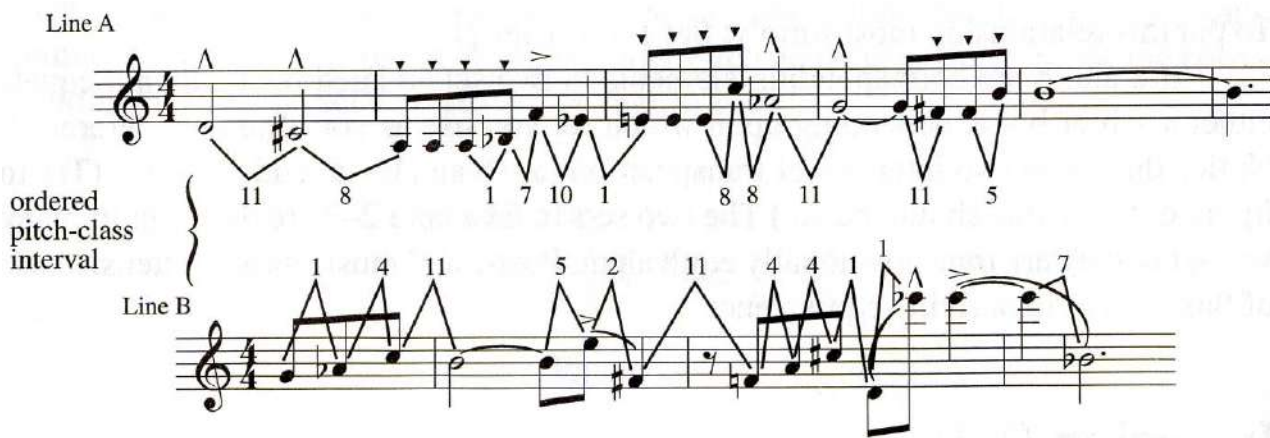


Figure 4: Two lines of pitch classes related by T9I (Schoenberg, String Quartet No. 4)

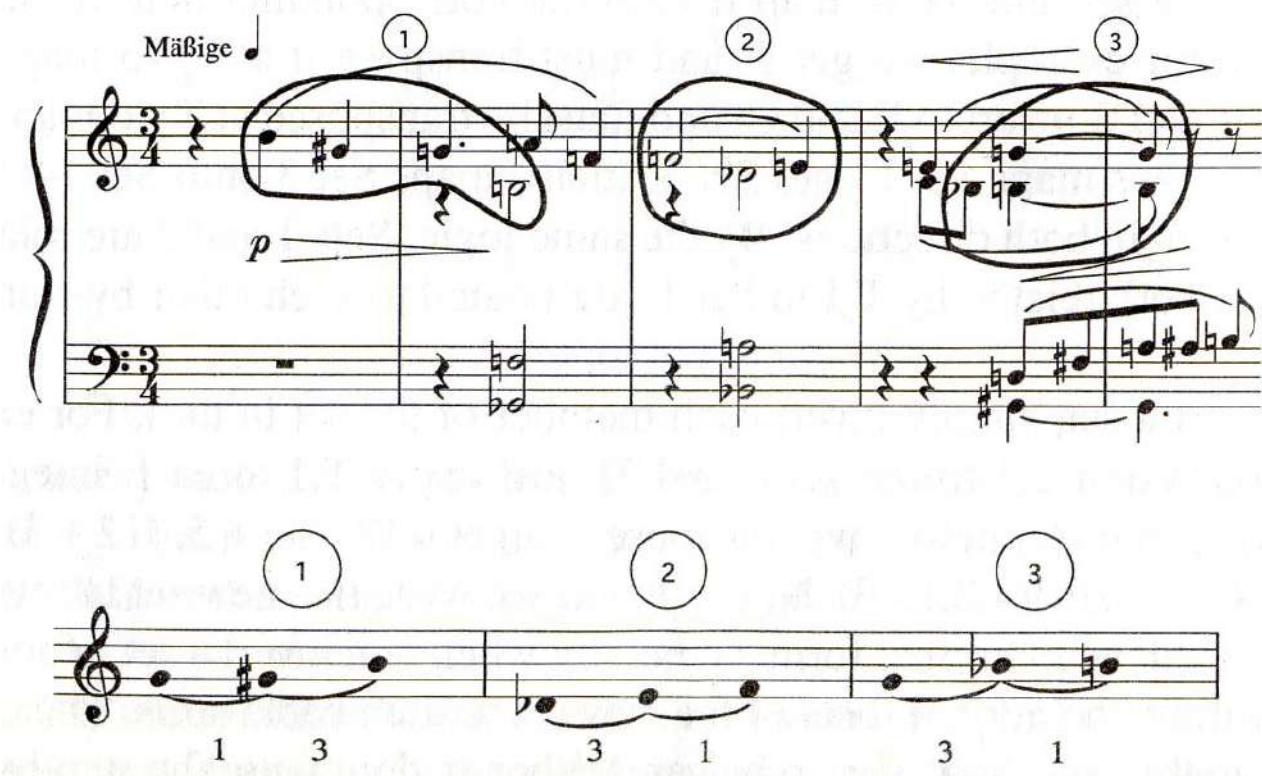


Figure 5: Inversionally equivalent pitch-class sets (Schoenberg, Piano Piece, Op. 11, No. 1)

5. A Flaw in Atonal Music Theory

Consider the operation that changes a major triad to a minor triad. To our ears, this is the same operation regardless of whether we start with a CM triad or a DM triad. However, consider the CM triad as the pitch class [047], cm as [037], DM as [269] and dm as [259]. Then, we have

$$\text{CM} \rightarrow \text{cm} = [047] \rightarrow [037] = \text{T7I} \quad \text{DM} \rightarrow \text{dm} = [269] \rightarrow [259] = \text{T11I}$$

This is a misleading representation of the music, because our ears do not hear two different actions. Therefore, the structure of atonal music theory has an inherent flaw. It cannot support these simple transformations.

A music theorist named Hugo Riemann recognized this problem. He invented the idea of a “triadic transformation.” Later music theorists devised three operations, called Neo-Riemannian operations, that functioned specifically on triads:

- The Parallel operation (P) moves the middle note of a triad up or down a semitone such that a major triad becomes minor and a minor triad becomes major. For example, it would move the E in a CM to an E \flat and the E \flat in a cm triad to an E \natural .
- The Leading-tone exchange (L) moves the bottom note of a major triad down a semitone and the top note of a minor triad up a semitone. Thus, a CM triad would turn into an em triad, and a cm triad would turn into an A \flat M triad.
- The Relative operation (R) sends a chord to its relative counterpart by moving the top note of a major triad up by a whole tone, and moving the bottom note of a minor triad down by a whole tone. Thus, a CM triad would turn into an am triad, and a cm triad would turn into an E \flat M triad.

These three were particularly interesting because they allowed for parsimonious voice-leading. That is, in moving from one triad to another, only one voice (top, middle or bottom) moved, and it moved by nothing more than a whole step. In addition, they allowed a transformation from any one chord to another by composition of these operations.

6. Uniform Triadic Transformations

This P, L and R notation, while a definite improvement, could still be unclear, unwieldy and limited in its usefulness. For example, a move from a CM triad to a b \flat m triad requires a minimum of six Neo-Riemannian operations. Furthermore, there are nine different ways to write it in six operations: LPRPR, LRPRP, PLRLR, PRLRP, PRPRL, RLPLR, RLRLP, RPLPR, RPRPL. Of course, there are even more ways to write it in more than six operations. Not only has this notation become pedantic, it also fails to reflect the music: who would hear six operations in a simple move from CM to b \flat m?

To resolve this problem, another music theorist named Julian Hook devised a new notation for transformations on triads, which he called uniform triadic transformations (UTTs). This notation, in fact, was a group structure with intriguing algebraic properties. Before we jump into a discussion on

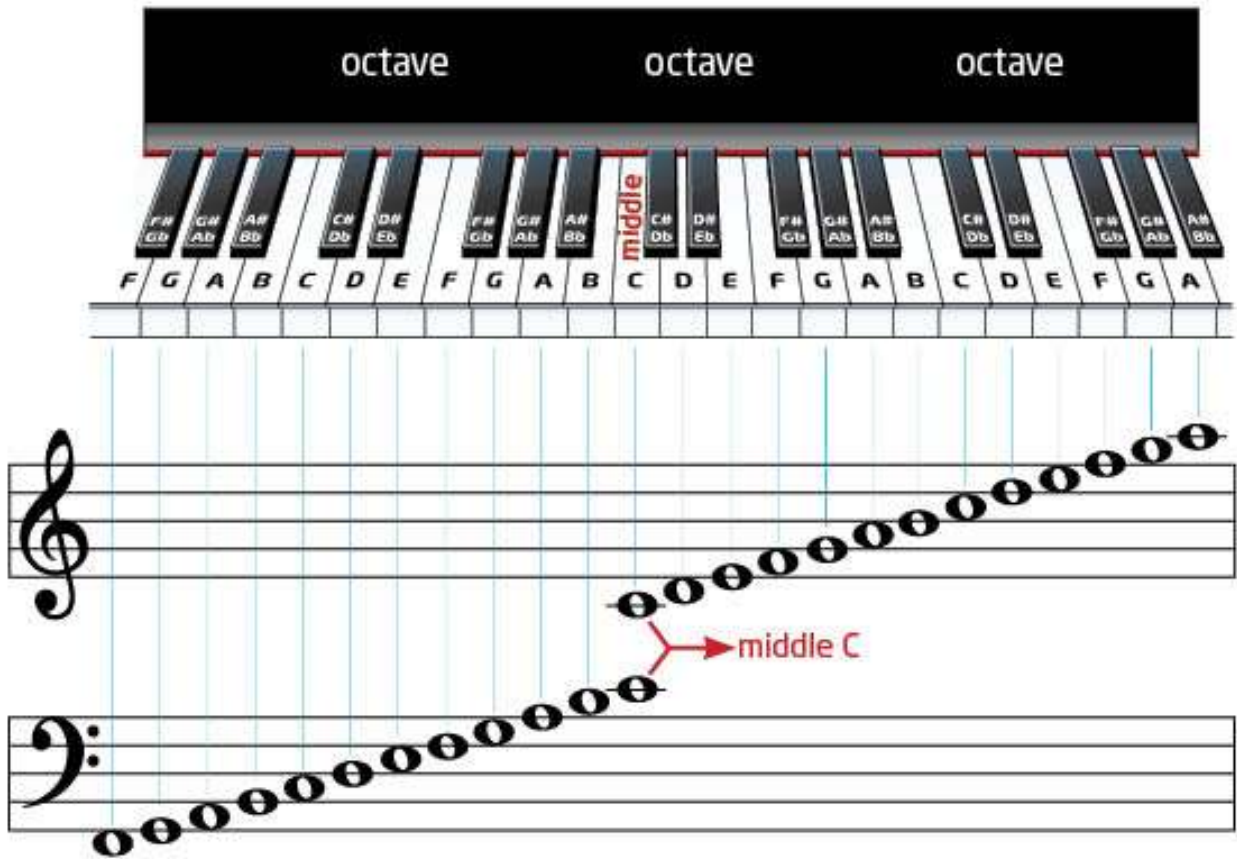


Figure 6: A piano with the keys placed onto the music staff

Definition 6.1. A triad is an ordered pair $\Delta = (r, \sigma)$ where r is the root of the triad expressed as an integer (mod 12), and σ is a sign representing its mode (+ for major, - for minor).

Example 6.2. $\Delta = (0, +)$ represents a C major triad and $\Delta = (6, -)$ represents an f# minor triad.

Theorem 6.3. The set of all 24 major and minor triads, forms a abelian group with multiplication defined by

$$(t_1, \delta_1)(t_2, \delta_2) = (t_1 + t_2, \delta_1\delta_2)$$

We call this set Γ .

Proof. This group is clearly isomorphic to $\mathbb{Z}_{12} \times \mathbb{Z}_2$, which by Theorem 2.23 is a group.

Definition 6.4. Given $\Delta_1 = (r_1, \delta_1)$ and $\Delta_2 = (r_2, \delta_2)$, the transposition level $t = r_2 - r_1$ is the interval between the roots and the sign factor $\delta = \delta_1\delta_2$ is the change in sign. (δ is multiplied as expected with $++ = +, +- = -, -+ = -$ and $-- = +$.) The Γ -interval $\text{int}(\Delta_1, \Delta_2)$ is the ordered pair (t, δ) where t and δ are the transposition level and sign factor as defined above.

Example 6.5. The Γ -interval from $(0, +)$ (C major) to $(6, -)$ (f# minor) is $(6, -)$.

6.1. Introduction to Triadic Transformations

Definition 6.6. A triadic transformation is a bijective mapping from Γ to itself. In other words, it is a permutation of Γ .

Theorem 6.7. The set of all triadic transformations forms a group G . Proof. After numbering the triads, this group is clearly isomorphic to S_{24} .

The order of G is huge: 24 factorial. However, most of these transformations have little musical meaning since the action of a transformation on one triad may not resemble its action on another triad.

6.2. V, the Uniform Triadic Transformations

Of particular musical interest are the UTTs because they operate on all major triads in the same manner. Similarly, the UTTs have one action for all minor triads.

Definition 6.8. Consider the triadic transformation that transforms (r, σ) to (r', σ') . It is a uniform triadic transformation (UTT) if it transforms $(r + t, \sigma)$ to $(r' + t, \sigma')$ $\forall t \in \mathbb{Z}_{12}$.

It is important to note that not all musically interesting transformations are UTTs. The inversions TnI , for example, are not part of the UTTs.

Any UTT is completely determined by three parameters:

- t^+ , its transposition level for a major triad
- t^- , its transposition level for a minor triad
- σ , its sign. (Note: it may seem that σ could be different for major and minor triads. However, in order to be a transformation, a UTT must map Γ to itself. Thus, if it switches major triads to minor, it must switch minor triads to major. That is $\delta^+ = -\delta^-$. Positive σ implies no change in mode (it is **mode-preserving**), negative σ implies switching to the opposite mode (it is **mode-reversing**).)

We can thus denote any UTT U by the ordered triple $U = \langle \sigma, t^+, t^- \rangle$. Example 6.9. We will convert Riemann's P, L and R in UTT notation:

$$P = \langle -, 0, 0 \rangle \quad L = \langle -, 4, 8 \rangle \quad R = \langle -, 9, 3 \rangle$$

Note, Hook uses left-to-right orthography. Thus, $U_1 U_2$ implies “first U_1 then U_2 .” As usual, $U^2 = U U$, etc. Although it is less intuitive for mathematicians, we will adhere to his notation.

6.2.1 Multiplication on V

Multiplication on V should clearly be composition. Before we derive a general formula for the composition of two UTTs, let us consider some concrete examples.

Example 6.10. Consider the UTTs $U = \langle +, 4, 7 \rangle$ and $V = \langle -, 5, 10 \rangle$. Let us calculate the product $UV = \langle \delta_{UV}, t_{UV}^+, t_{UV}^- \rangle$. When UV acts on a CM triad ($\Delta = (0, +)$) we have:

$$(0, +) \xrightarrow{U} (4, +) \xrightarrow{V} (9, -)$$

Thus, UV transforms the major triads through the Γ -interval (9, -). We can deduce that $\delta_{UV} = -$ and $t_{UV}^+ = 9$.

When UV acts on a cm triad ($\Delta = (0, -)$) we have:

$$(0, -) \xrightarrow{U} (7, -) \xrightarrow{V} (5, +)$$

Thus, UV transforms the minor triads through the Γ -interval (5, +) and $t_{UV}^- = 5$. Hence, $UV = \langle -, 9, 5 \rangle$

This product may be calculated by multiplying the signs ($\delta_{UV} = \delta_U \delta_V$) and adding the corresponding transposition levels ($t_{UV}^+ = t_U^+ + t_V^+$; $t_{UV}^- = t_U^- + t_V^-$). Figure 6 depicts a visual representation of UV.

Example 6.11. Now consider the product VU. In this case we have

$$(0, +) \xrightarrow{V} (5, -) \xrightarrow{U} (0, -)$$

and

$$(0, -) \xrightarrow{V} (10, +) \xrightarrow{U} (2, +)$$

Therefore, $VU = \langle -, 0, 2 \rangle$. In this case, the signs were multiplied as before, the transposition levels were “cross-added.” That is, $t_{UV}^+ = t_U^+ + t_V^-$ and $t_{UV}^- = t_V^+ + t_U^-$.

We can see that in the above example, the “cross-adding” was due to the sign of the first transformation. In the first case, the first UTT (U) was mode-preserving, so the second UTT (V) acted on the same mode as U. Thus, the corresponding transposition levels were applied in succession. In the second case, the first UTT (V) was mode-reversing, so the second UTT (U) acted on the opposite mode as V and opposite transposition levels were combined. This leads us to the general form of UTT multiplication:

Theorem 6.12. Consider two UTTs $U = \langle \delta_U, t_U^+, t_U^- \rangle$ and $V = \langle \delta_V, t_V^+, t_V^- \rangle$. Multiplication on V is given by $UV = \langle \delta_U \delta_V, t_U^+ + t_V^{(\delta_U)}, t_U^- + t_V^{(-\delta_U)} \rangle$

The reader can verify that following the process above using two arbitrary elements in V will give the desired result.

6.2.2 Inversion on V

Again, before we derive a general formula for the inverse of a UTT, let us consider some concrete examples.

Example 6.13. Consider the UTT $U = \langle +, 4, 7 \rangle$. Because $(0, +) \xrightarrow{U} (4, +)$ and $(0, -) \xrightarrow{U} (7, -)$, we need $(4, +) \xrightarrow{U^{-1}} (0, +)$ and $(7, -) \xrightarrow{U^{-1}} (0, -)$. Thus, $U^{-1} = \langle +, 8, 5 \rangle$. Note how this is simply the inversion of the transposition levels: $\langle +, -4 \pmod{12}, -7 \pmod{12} \rangle$.

Example 6.14. Now consider the UTT $V = \langle -, 5, 10 \rangle$. $(0, +) \xrightarrow{V} (5, -)$ and $(0, -) \xrightarrow{V} (10, +)$. Thus, $(5, -) \xrightarrow{V^{-1}} (0, +)$ and $(10, +) \xrightarrow{V^{-1}} (0, -)$. Therefore, $V^{-1} = \langle -2, 7 \rangle$ or $\langle -, -10 \pmod{12}, -5 \pmod{12} \rangle$. In this case, the transposition levels are not only inverted, but interchanged. Once again, this is due to the sign of V.

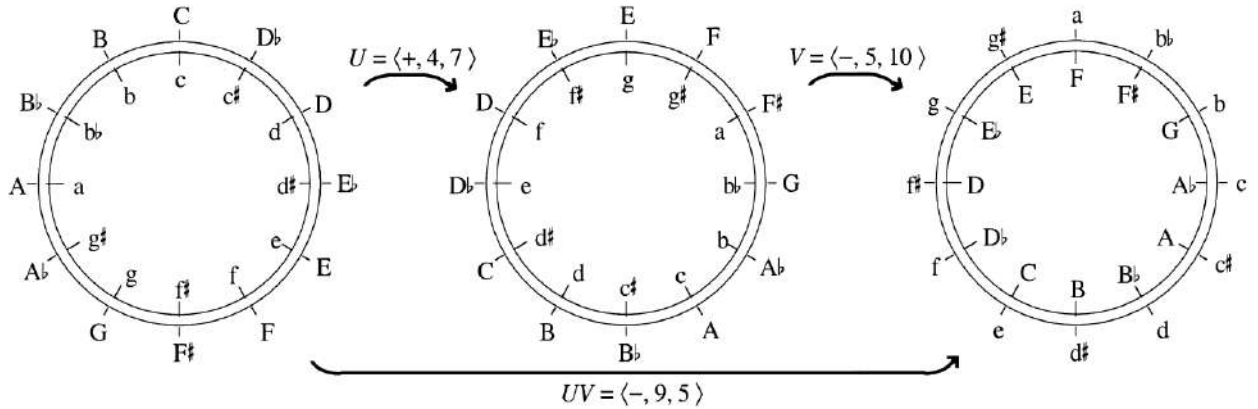


Figure 7: Visual representation of the UTT equation $\langle +, 4, 7 \rangle \langle -, 5, 10 \rangle = \langle -, 9, 5 \rangle$

Theorem 6.16. The set V of UTTs is a group that is isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$

Proof. Remember from Section 2.4.3 how we represented $G \times G$ in the form $r_1^m r_2^n$. Let G be \mathbb{Z}_{12} and let us switch the 1 and 2 to + and -. Then the elements of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ are $s r_+^m r_-^n$ where $m, n \in \mathbb{Z}_{12}$.

Also note that the transpositions, which are equivalent to the transposition levels of a UTT, are isomorphic to the rotations of the D_{12} by $T_n \rightarrow r^n$. We initially wrote that the $T_n/T_n I$ group was isomorphic by $T_n \rightarrow r^{12-n}$. This reflected our visual representation of the two groups. However, the groups are still isomorphic if we choose $T_n \rightarrow r^n$, which makes the following argument clearer.

It seems likely that the UTTs are isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ by $\langle \sigma, t^+, t^- \rangle \rightarrow s r_+^m r_-^n$. We have already shown that the UTTs have multiplication and inverses. We only need to show that it follows the multiplication of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$. That is, $(r_+^m r_-^n)s = s(r_-^n r_+^m)$.

$$\begin{aligned}
 (r_+^m r_-^n)s &= (e r_+^m r_-^n)(see) \\
 &= \langle -, 0, 0 \rangle \langle +, t_m^+, t_n^- \rangle \\
 &= \langle -, 0 + t_n^-, 0 + t_m^+ \rangle \\
 &= \langle -, t_n^-, t_m^+ \rangle \\
 &= s(r_-^n, r_+^m)
 \end{aligned}$$

Thus, multiplication is preserved and the isomorphism holds.

6.2.3 Even and Odd UTTs

UTTs can be classified as “even” or “odd” in multiple ways. Let us begin with “even/odd in the sense of total transposition.”

Definition 6.17. We say that a UTT $U = \langle \sigma, t^+, t^- \rangle$ is even (or, more fully, even in the sense of total transposition) if its total transposition $\tau(U) = t^+ + t^-$ is an even number. U is odd (in the sense of total transposition) if $\tau(U)$ is an odd number.

Definition 6.19. A UTTs is even (in the sense of permutation theory) if it can be written as a product of an even number of 2-cycles and odd (in the sense of permutation theory) if it can be written as a product of an odd number of 2-cycles.

It is remarkable that the two definitions of even or odd (in the sense of total transposition versus permutation theory) are actually equivalent.

Theorem 6.20. A UTT is even in the sense of total transposition if and only if it is even in the sense of permutation theory.

6.3. \mathbb{R} , the Riemannian UTTs

Recall the Neo-Riemannian operators P , L and R as introduced in Section 5 and written as UTTs in Example 6.9. For each, the transposition level for a major triad is equal and opposite that of a minor triad. We define the Riemannian UTTs as follows.

Definition 6.21. A Riemannian UTT is a UTT such that $t^+ = -t^-$.

Theorem 6.22. The set of \mathbb{R} of Riemannian UTTs is isomorphic to D_{12} .

Proof. D_{12} can be defined as the group of order 24 generated by s and r , such that $s^2 = e$, $r^{12} = e$ and $sr = r^{-1}s$

The generators of \mathbb{R} are $\langle -, 0, 0 \rangle$ and $\langle +, 1, 11 \rangle$.

$$(\langle -, 0, 0 \rangle)^2 = \langle -, 0+0, 0+0 \rangle = \langle +, 0, 0 \rangle = e \in \mathbb{R}$$

$$(\langle +, 1, 11 \rangle)^{12} = \langle +, 12 \cdot (1), 12 \cdot (11) \rangle = \langle +, 0, 0 \rangle = e$$

$$(\langle +, 1, 11 \rangle)^{-1} = \langle +, 11, 1 \rangle$$

$$\langle -, 0, 0 \rangle \langle +, 1, 11 \rangle = \langle -, 0 + 11, 0 + 1 \rangle = \langle -, 11 + 0, 1 + 0 \rangle$$

$$= \langle +, 1, 11 \rangle \langle -, 0, 0 \rangle = r^{-1}s$$

6.4 \mathbb{K} , the Subgroups of \mathbb{V}

Generally, it is difficult to list all the subgroups of a given group G . However, it is possible to list all the subgroups of \mathbb{V} .

Definition 6.23. Give two integers a and b (mod 12), we define three subsets of \mathbb{V} as follows.

- $K^+(a)$ is the set of all mode-preserving UTTs of the form $\langle +, n, an \rangle$ as n ranges through the integers mod 12.

- $K^-(a, b)$ is the set of all mode-reversing UTTs of the form $\langle -, n, an+b \rangle$.
- $K(a, b) = K^+(a) \cup K^-(a, b)$

Theorem 6.24. $K(a, b)$ is a subgroup of V if and only if the numbers a and b satisfy $a^2=1$ and $ab = b \pmod{12}$.

The condition $a^2 = 1$ is satisfied only for $a = 1, 5, 7$ and 11 . If $a = 1$ then the condition $ab = b$ is automatically satisfied. For other values of a , the allowable values of b are different in each case. The following is a complete list of the groups $K(a, b)$:

$K(1,0), K(1,1), K(1,2), \dots, K(1,11)$
 $K(5, 0), K(5, 3), K(5, 6), K(5, 9)$
 $K(7, 0), K(7, 2), K(7, 4), K(7, 6), K(7, 8), K(7, 10) K(11, 0), K(11, 6)$

7. Musical Application

The UTTs of order 24 are of considerable musical interest. When such a transformation is applied repeatedly, the resulting chain of triads will cycle through all 24 major and minor triads before returning to the original one. Take, for example, the UTT $U = \langle -, 9, 8 \rangle$. Its repeated application produces a chain in the scherzo of Beethoven's Ninth Symphony :

$$C \xrightarrow{U} a \xrightarrow{U} F \xrightarrow{U} d \rightarrow \dots \xrightarrow{U} A$$

This chain is 19 triads long, only five short of a complete cycle.

Such triad chains are rarely prolonged to this extent. There are, however, examples from literature that circumnavigate the entire cycle of 24 triads. These are found in collections of pieces such as Bach's Well-Tempered Clavier and the Chopin Preludes.

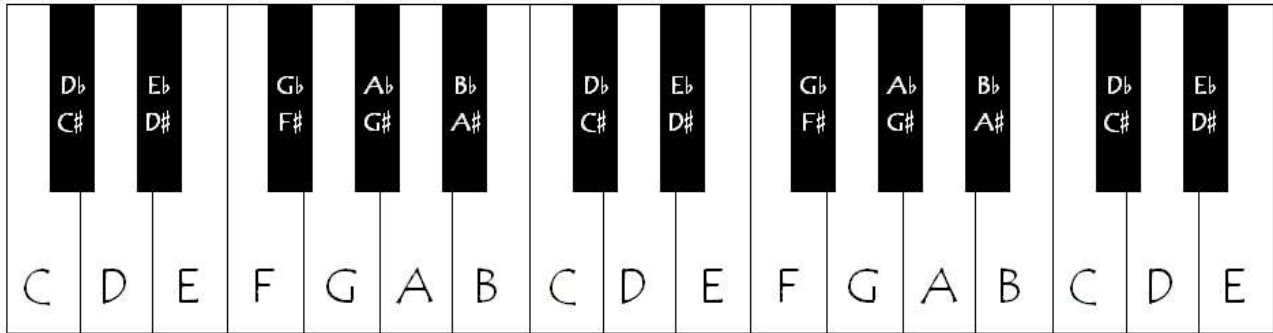


Figure 8: A piano with the keys labeled

8. Conclusion

We can see that Hook's UTTs not only have interesting mathematical properties, but also musical significance. Musically, the choice of triads is non-arbitrary since triads occur throughout music. Mathematically, however, the set choice is arbitrary. Some current research in music theory investigates the generalization Hook's UTTs to larger chords or even to pitch-class sets. The flexibility these generalisations will provide may greatly improve atonal analysis.

References

- [1] Armstrong, M. Groups and Symmetry. Springer-Verlag, 1988.
- [2] Dummit, D. S., and Foote, R. M. Abstract Algebra, third ed. Wiley, 2003.
- [3] Hook, J. Uniform triadic transformations. *Journal of Music Theory* 46, 1-2 (2002), 57–126.
- [4] Straus, J. N. Introduction to Post-Tonal Theory, second ed. Prentice-Hall, Inc., 2000.

Shubhajit Bhowmick

Registration No : A01-1152-113-057-2017

Roll no : 1374

Semester : 5

Paper : CC-12

**Topic : The Framework of Music Theory as
Represented with Groups**

Acknowledgement

I would like to express my special thanks of gratitude to our beloved **Pravanjan Kumar Rana Sir** who gave me the opportunity to do this wonderful project on the topic **The Framework of Music Theory as Represented with Groups**, which also helped me in doing a lot of research and I come to know about so many new things.

Secondly I would like to thank my friends **Pranay Mandal** and **Satyabrata Pradhan** who helped me a lot in finishing this project within the limited. It helped me increase my knowledge and skills.

The Framework of Music Theory as Represented with Groups

Contents

- 1 Introduction
- 2 Basic Group Theory
 - 2.1 What is a group ?
 - 2.2 Permutations
 - 2.3 Morphisms
 - 2.3.1 Homomorphisms
 - 2.3.2 Isomorphisms
 - 2.3.3 Automorphisms
 - 2.4 Products
 - 2.4.1 Direct Products
 - 2.4.2 Semidirect Products
 - 2.4.3 Wreath Products
- 3 Music Theory
 - 3.1 Basic concepts of atonal music theory
 - 3.1.1 T_n , the Transpositions
 - 3.1.2 $T_n I$, the Inversions
- 4 Group Theory as a Structure for Atonal Music Theory
- 5 A Flaw in Atonal Music Theory
- 6 Uniform Triadic Transformations

6.1 Introduction to Triadic Transformations

6.2 V , the Uniform Triadic Transformations

6.2.1 Multiplication on V

6.2.2 Inversion on V

6.2.3 Isomorphism to $Z_{12} \wr Z_2$

6.2.4 Even and Odd UTTs

6.3 R , the Riemannian UTTs

6.4 K , the Subgroups of V

7 Musical Application

8 Conclusion

References

1. Introduction

In 2002, a music theorist by the name of Julian Hook published a paper in the Journal of Music Theory titled, “Uniform Triadic Transformations.” In this paper, Hook generalized some existing music theoretical concepts and greatly improved their notation. Hook’s UTTs formed a group with interesting algebraic properties.

This paper will first give the reader a review of all necessary group theory to understand the discussion of Hook’s UTTs. Then it will review music theory (atonal theory in particular) and its evolution to the UTTs. Finally, it will discuss the UTTs themselves and conclude with some musical applications.

2 . Basic Group Theory

Group theory is a branch of mathematics that studies groups. This algebraic structure forms the basis for abstract algebra, which studies other structures such as rings, fields, modules, vector spaces and algebras. These can all be classified as groups with addition operations and axioms.

This section provides a quick and basic review of group theory, which will serve as the basis for discussions in the group theoretical structure as applied to music theory.

2.1 . What is a group?

A group is a set such that any two elements x and y can be combined via “multiplication” to form a unique product xy that also lies in the set. This multiplication is defined for every group and does not necessarily refer to the traditional meaning of “multiplication.” We now state the formal definition of a group:

Definition 2.1. A group is a set G together with a multiplication on G which satisfies three axioms:

- (a) The multiplication is associative, that is to say $(xy)z = x(yz)$ for any three (not necessarily distinct) elements in G .
- (b) There is an element $e \in G$, called an identity element, such that $xe = e = ex, \forall x \in G$
- (c) Each element $x \in G$ has an inverse x^{-1} which belongs to the set G and satisfies $x^{-1}x = e = xx^{-1}$

Theorem 2.2. Every group G satisfies the following properties:

- (a) The identity element e of G is unique
- (b) $\forall x \in G$, the inverse x^{-1} is unique

Note how commutativity of the multiplication is not required within a group. Therefore, we define an abelian group as follows:

Definition 2.3. A group G is abelian if its multiplication is commutative. That is, $xy = yx$ for any two elements in G .

To better illustrate the concept of a group, we now give some examples. Example 2.4. The reals excluding 0, $\mathbb{R} \setminus \{0\}$ under multiplication:

- The group is closed under multiplication: $\forall x, y \in \mathbb{R}, x \cdot y \in \mathbb{R}$

- The multiplication is associative: $\forall x, y, z \in \mathbb{R}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- The identity is 1: $\forall x \in \mathbb{R}, 1 \cdot x = x \cdot 1$
- The inverse of x is $\frac{1}{x}$: $\frac{1}{x} \cdot x = 1 = x \cdot \frac{1}{x}$

This group is abelian since $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$. Note how we must exclude 0 for this to be a group since there exists no inverse for 0. That is, there does not exist some $x \in \mathbb{R}$ such that $x \cdot 0 = 1$

Example 2.4. The integers $\mathbb{Z} \pmod{12}$, which we will denote as \mathbb{Z}_{12} , under addition $\pmod{12}$. (Note: in abstract algebra, $\mathbb{Z} \pmod{12}$ is generally notated as $\mathbb{Z}/(12)$ and \mathbb{Z}_{12} refers to another algebraic structure. However, in music theory, only $\mathbb{Z} \pmod{12}$ is of significance and we will use this more concise notation.)

- The group is closed under addition $\pmod{12}$: for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y \in \mathbb{Z}_{12}$.
- Addition $\pmod{12}$ is associative.
- The identity is 0.
- The inverse of x is $12-x$.

This group is also abelian since for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y = y +_{12} x$.

Example 2.6. The dihedral groups represent the symmetries of a regular polygon that map it onto itself. Consider the regular hexagon. Let r denote the rotation of through $\pi/3$ about the axis of symmetry perpendicular to the hexagon (rotating), let s denote the rotation through π about an axis of symmetry that lies in the plane of the plate (flipping), and let e denote the identity (leaving the hexagon unchanged). Then the dihedral group D_6 consists of the following 12 elements.

It may seem that the group is not closed under multiplication since the element sr is missing from the group. However, a rotation r takes the hexagon. A subsequent flip s takes the hexagon. Thus, rs is equivalent to r^5s . The reader can check that the whole group is indeed closed under multiplication. In general,

$$sr^n = r^{6-n}s, \forall n \in \mathbb{Z}_6$$

for the D_6 dihedral group.

Definition 2.7. The order of a group is the number of elements in the group.

Definition 2.8. The order of some element x of a group G is the smallest positive integer n such that $x^n = e$.

Definition 2.9. A subgroup of a group G is a subset of G which itself forms a group under the multiplication of G

Definition 2.10. A group G is cyclic if there exists an $x \in G$ such that for all $y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$. We call x a generator of G .

Definition 2.11. A permutation of an arbitrary set X is a bijection from X to itself.

Permutations can be denoted in multiple ways. Consider r from the D_6 dihedral group. We can represent it as a permutation of integers like so: (054321) , where each integer is sent to the one following it, and the final one is sent to the first. Likewise, we can write sr as $(01)(25)(34)$.

Definition 2.12. A permutation of the form $(a_1 a_2 \dots a_k)$ is called a cyclic permutation. A cyclic permutation of length k is called a k -cycle.

Definition 2.13. A transposition is 2-cycle. Any k -cycle $(a_1 a_2 \dots a_k)$ can be written as a product of transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$$

Note that transpositions may be written as many different products. This product is not unique, but is meant to show the existence of a product consisting only of transpositions.

Definition 2.14. An even permutation is a permutation that can be written as an even number of transpositions. The others are called odd permutations.

It may bother the reader that the a permutation in the form of a product of transpositions is not unique. Perhaps a permutation could be written as both an even number of transpositions and an odd number. However, the following theorem shows that the definition is well defined.

Theorem 2.15. Although any permutation can be written as a product of transpositions in infinitely many different ways, the number of transpositions which occur is always even or always odd.

Theorem 2.16. Consider the set X of n elements. The set of all permutations of X forms a group S_n called the symmetric group of degree n . Multiplication on this group is defined by composition of functions.

2.3 Morphisms

2.3.1 Homomorphisms

Definition 2.17. Let G and G' be groups. A homomorphism is a function $\phi : G \rightarrow G'$ that preserves the multiplication of G . Therefore, $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$

Example 2.18. Let ϕ be a function from D_{12} to Z_2 defined by $\psi(r^n) = 0$ and $\psi(r^n s) = 1$. Consider two elements x and y in D_{12} . We have four cases:

$$\bullet x = r^m, y = r^n;$$

$$\psi(xy) = \psi(r^m r^n) = \psi(r^{m+n}) = 0 = 0 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n;$$

$$\psi(xy) = \psi(r^m s r^n) = \psi(r^{m-n} s) = 1 = 1 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m, y = r^n s;$$

$$\psi(xy) = \psi(r^m r^n s) = \psi(r^{m+n} s) = 1 = 0 + 1 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n s;$$

$$\psi(xy) = \psi(r^m s r^n s) = \psi(r^{m-n} ss) = \psi(r^{m-n}) = 0 = 1 + 1 = \psi(x)\psi(y)$$

Hence, ϕ satisfies the properties of a homomorphism.

2.3.2 Isomorphisms

Definition 2.19. An isomorphism is a bijective homomorphism.

Example 2.20. \mathbb{Z}_{12} is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$. Consider the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$(0,0) \quad (0,1) \quad (0,2) \quad (0,3)$$

$$(1,0) \quad (1,1) \quad (1,2) \quad (1,3)$$

$$(2,0) \quad (2,1) \quad (2,2) \quad (2,3)$$

Send each element (x, y) to $4x + y$ and you have \mathbb{Z}_{12}

2.3.3 Automorphisms

Definition 2.21. An automorphism of a group G is an isomorphism from G to G . The set of all automorphisms forms a group under composition of functions, which is called the automorphism group of G and written $\text{Aut}(G)$.

Automorphisms fix the identity and send generators to generators.

Example 2.22. Consider the automorphisms of \mathbb{Z}_4 . There are only two generators in this group: 1 and 3. Therefore, there are only two elements in $\text{Aut}(\mathbb{Z}_4)$: the trivial one, and the one that flips 1 and 3.

2.4 Products

2.4.1 Direct Products

Theorem 2.23. The set $G \times H$ of two groups G and H is a group that consists of the elements (g, h) where $g \in G$ and $h \in H$. Given two elements (g, h) and (g', h') of $G \times H$, multiplication on this group is defined by

$$(g, h)(g', h') = (gg', hh')$$

where the first term, gg' , inherits the multiplication of G , and the second, hh' , inherits the multiplication of H . We call this group the direct product $G \times H$ of G and H .

Proof. Associativity follows from the associativity in both G and H . The identity is (e, e) and the (g^{-1}, h^{-1}) is the inverse of (g, h) .

Example 2.24. Consider $\mathbb{Z}_4 \times \mathbb{Z}_2$. This group has 8 elements: $(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)$.

Multiplication is defined by

$$(x, y) + (x', y') = (x + 4x', y + 2y')$$

2.4.2. Semidirect Products

Theorem 2.25. Suppose we have the groups G, H and the homomorphism $\phi : G \rightarrow \text{Aut}(H)$. Then the “twisted” direct product forms a new group. Its elements are of the form (g, h) with $g \in G$ and $h \in H$ and multiplication is defined by

$$(g, h)(g', h') = (g \cdot \phi(h)(g'), h \cdot h').$$

We call this group the semidirect product of G and H .

Example 2.26. Consider the semidirect product $\mathbb{Z}_4 * \mathbb{Z}_2$. The elements in this group are the same as those in $\mathbb{Z}_4 \times \mathbb{Z}_2$ as listed in Example 2.24.

We need to define ϕ . There are only two automorphisms of \mathbb{Z}_4 as shown in Example 2.22. Let the trivial automorphism be denoted with e and the other with σ . Then, since $\phi: \mathbb{Z}_2 \rightarrow \text{Aut}(H)$, we have $\phi(0) = e$ and $\phi(1) = \sigma$.

Now we can perform multiplication on the group. Consider multiplying the elements $(0, 0)$ and $(1, 0)$. Since $\phi(0) = e$ this multiplication is just like that of the direct product:

$$(0, 0)(1, 0) = (0 + \phi(0)1, 0 + 0) = (0 + e(1), 0 + 0)(1, 0)$$

Now consider the elements $(1, 0)$ and $(0, 1)$.

$$(0, 1)(1, 0) = (0 + \phi(1)(1), 1 + 0) = (0 + \sigma(1), 1 + 0) = (3, 1)$$

2.4.3. Wreath Products

The generalized form of a wreath product $G \wr H$ is too complicated for the scope of this paper. Therefore, we will only consider the special case taking a wreath product with \mathbb{Z}_2 .

Consider the group G . Then $G \wr \mathbb{Z}_2$ is isomorphic to $(G \times G) * \mathbb{Z}_2$. We will discuss this semidirect product in the dihedral notation as in Example 2.27. Thus, let the elements of $G \times G$ be denoted by $r_1^m r_2^n$.

The automorphism for a wreath product must permute the parts of an element in $G \times G$. Since we only have two elements, r_1^m and r_2^n , the only non-trivial automorphism is to switch them. That is $\delta(r_1^m r_2^n) = r_2^n r_1^m$. Thus,

$$r_1^m r_2^n s = s \delta(r_1^m r_2^n) = s r_2^n r_1^m$$

3. Music Theory

Music theory is a tool and framework with which we explain our listening experience. However, both the tool and the term “listening experience” are loosely defined. They are dependent on the music.

During the mid-15th century, composers began constructing their pieces around a particular pitch, called the tonic. This pitch was quickly established at the start of the piece and all other pitches were heard relative to it. Intervals and chords were labeled as consonant or dissonant. A feeling of tension occurred in various ways, such as when resolution was delayed, or when the music leapt to

distant keys (more than two accidentals removed from the tonic). Resolution to the tonic was crucial to ending the piece. After over two centuries of tonal music, listeners have begun to expect music to resolve in particular ways.

Along with the development of tonal music was the development of tonal theory. Its structure and notation allowed theorists to describe the listener's expectation. Thus, it provided an explanation for our reaction to particular harmonies. It explained our feeling of surprise at a particular chord and our feeling of finality at the end of a piece.

Around the turn of the 19th century, composers pushed the boundaries of tonal music. They began using dissonant chords with unprecedented freedom and resolved them in new ways. Eventually, their pieces no longer fit the framework of tonal music. Tonal theory no longer provided an adequate explanation for our listening experience. Thus, a new framework was constructed called atonal music theory.

Discussions in music require a certain vocabulary. The following terms are defined in the appendix:

- interval
- half step (semitone) & whole step (whole tone), flat, sharp, natural & accidental
- enharmonic equivalence
- major, minor, mode
- parallel & relative
- scale degree
- triad

3.1. Basic concepts of atonal music theory

Atonal music is based on sequences of pitches and intervals. No particular pitch is considered more important than the others and resolution of dissonance is unimportant. It assumes octave and enharmonic equivalence.

Definition 3.1. Pitches that are separated by an integer multiple of an octave, or are enharmonically equivalent belong to the same pitch class.

Definition 3.2. Consider the pitches a and b . The ordered pitch-class interval from a to b is $a-b \pmod{12}$.

Definition 3.3. A pitch-class set is an unordered set of pitch-classes, denoted as a string of integers enclosed in brackets. Within a pitch-class set, we do not have information about the register, rhythm or order of the pitches.

Example 3.4. The C major triad consists of the notes C, E and G. This can be represented as the pitch-class set [047], since $C = 0$, $E = 4$ and $G = 7$.

In atonal music, operations are performed on pitch-class sets, creating new pitch-class sets that are spread throughout the music. Thus, the music sounds random and yet structured at the same time. We will discuss two types of operations in this paper: the transpositions and the inversions.

3.1.1 T_n , the Transpositions

Definition 3.5. The transposition T_n moves a pitch-class or pitch-class set up by $n \pmod{12}$. (Note: moving down by n is equivalent to moving up by $12-n$.)

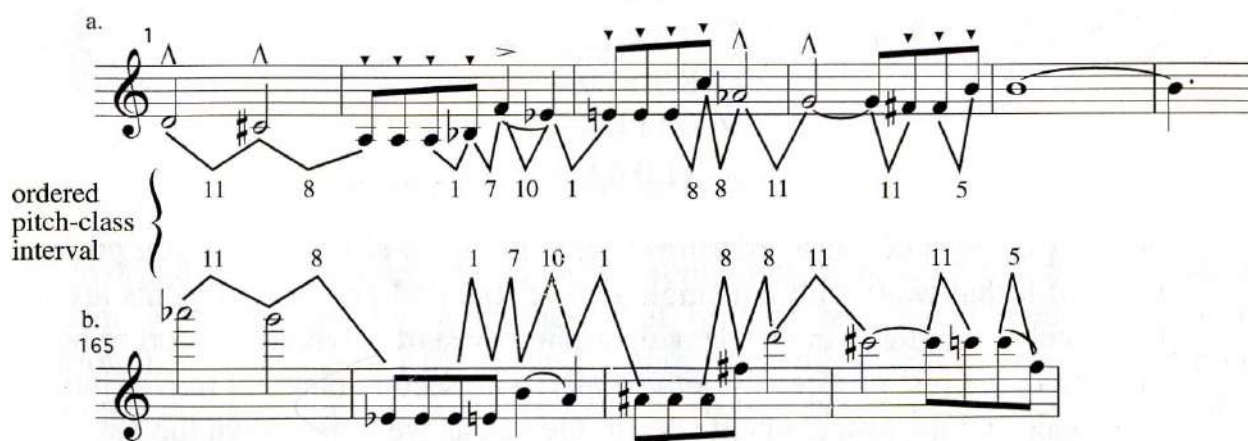


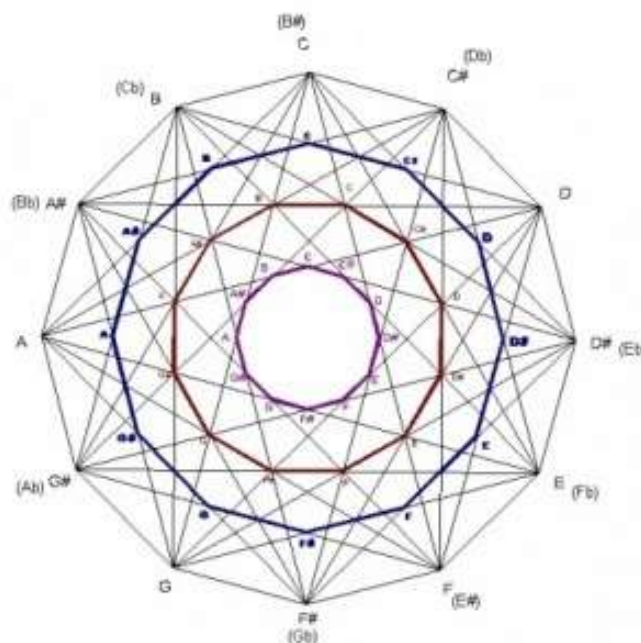
Figure 1: Two lines of pitch classes related by T6 (Schoenberg, String Quartet No. 4).

3.1.2 TnI, the Inversions

Definition 3.6. Consider the pitch a . Inversion $T_n I$ inverts the pitch about $C(0)$ and then transposes it by n . That is, $T_n I(a) = -a + n(\text{mod } 12)$.

4. Group Theory as a Structure for Atonal Music Theory

The numbering of the pitch classes reveals their isomorphism to \mathbb{Z}_{12} . More interestingly, the group of transpositions and inversions, denoted $T_n/T_n I$ is isomorphic to the dihedral group D_{12} .



Sehr langsam $\text{♩} = \text{ca. } 40$

Fl.

Ob.

Cl.

Trp.

Vln.

Vla.

Piano

1

2

3

4

Immer mit Dmpf.

mit Dmpf.

pp

p

Figure 3: Transpositionally equivalent pitch-class sets (Webern, Concerto for Nine Instruments, Op. 24).

Line A

ordered pitch-class interval

Line B

Figure 5: Inversionally equivalent pitch-class sets (Schoenberg, Piano Piece, Op. 11, No. 1)

5. A Flaw in Atonal Music Theory

Consider the operation that changes a major triad to a minor triad. To our ears, this is the same operation regardless of whether we start with a CM triad or a DM triad. However, consider the CM triad as the pitch class [047], cm as [037], DM as [269] and dm as [259]. Then, we have

$$\text{CM} \rightarrow \text{cm} = [047] \rightarrow [037] = \text{T7I} \quad \text{DM} \rightarrow \text{dm} = [269] \rightarrow [259] = \text{T11I}$$

This is a misleading representation of the music, because our ears do not hear two different actions. Therefore, the structure of atonal music theory has an inherent flaw. It cannot support these simple transformations.

A music theorist named Hugo Riemann recognized this problem. He invented the idea of a “triadic transformation.” Later music theorists devised three operations, called Neo-Riemannian operations, that functioned specifically on triads:

- The Parallel operation (P) moves the middle note of a triad up or down a semitone such that a major triad becomes minor and a minor triad becomes major. For example, it would move the E in a CM to an E \flat and the E \flat in a cm triad to an E \natural .
- The Leading-tone exchange (L) moves the bottom note of a major triad down a semitone and the top note of a minor triad up a semitone. Thus, a CM triad would turn into an em triad, and a cm triad would turn into an A \flat M triad.
- The Relative operation (R) sends a chord to its relative counterpart by moving the top note of a major triad up by a whole tone, and moving the bottom note of a minor triad down by a whole tone. Thus, a CM triad would turn into an am triad, and a cm triad would turn into an E \flat M triad.

These three were particularly interesting because they allowed for parsimonious voice-leading. That is, in moving from one triad to another, only one voice (top, middle or bottom) moved, and it moved by nothing more than a whole step. In addition, they allowed a transformation from any one chord to another by composition of these operations.

6. Uniform Triadic Transformations

This P, L and R notation, while a definite improvement, could still be unclear, unwieldy and limited in its usefulness. For example, a move from a CM triad to a b \flat m triad requires a minimum of six Neo-Riemannian operations. Furthermore, there are nine different ways to write it in six operations: LPRPR, LRPRP, PLRLR, PRLRP, PRPRL, RLPLR, RLRLP, RPLPR, RPRPL. Of course, there are even more ways to write it in more than six operations. Not only has this notation become pedantic, it also fails to reflect the music: who would hear six operations in a simple move from CM to b \flat m?

To resolve this problem, another music theorist named Julian Hook devised a new notation for transformations on triads, which he called uniform triadic transformations (UTTs). This notation, in fact, was a group structure with intriguing algebraic properties. Before we jump into a discussion on

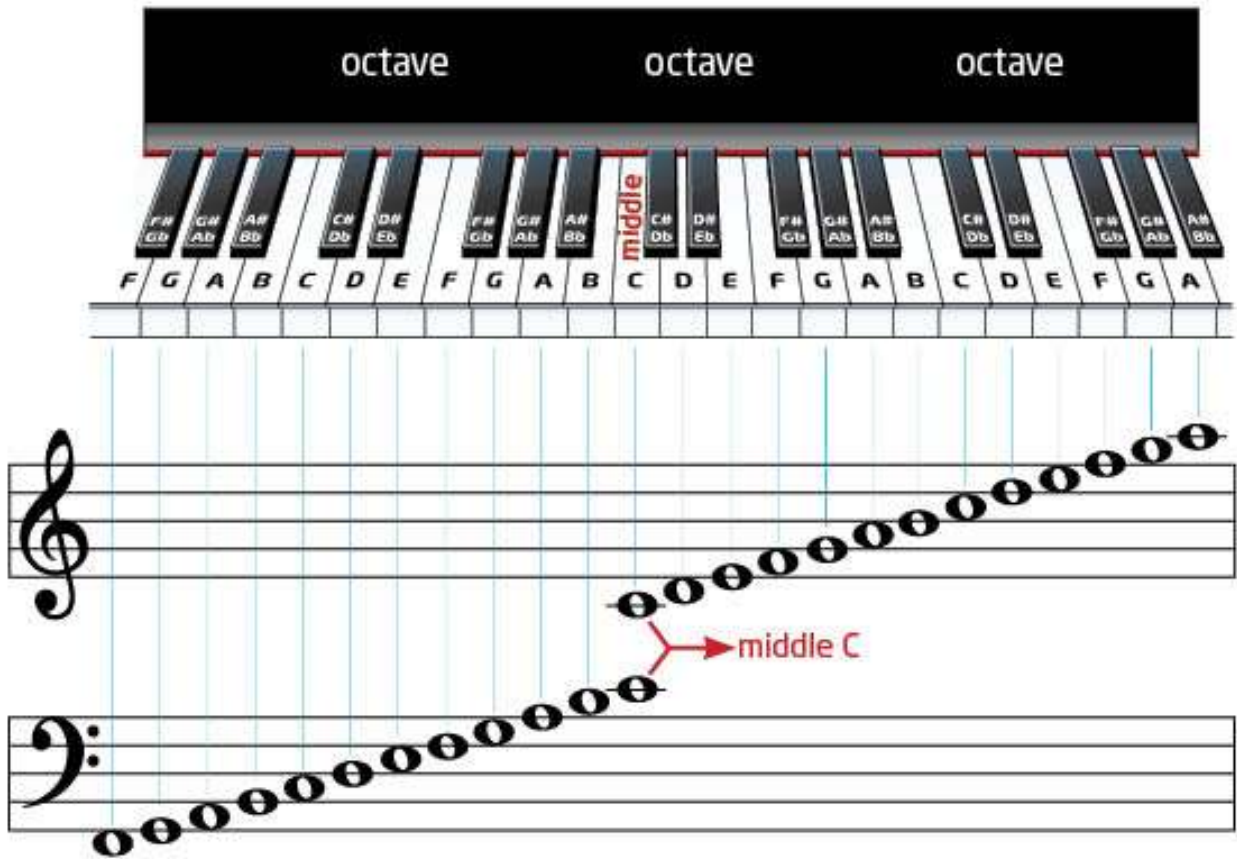


Figure 6: A piano with the keys placed onto the music staff

Definition 6.1. A triad is an ordered pair $\Delta = (r, \sigma)$ where r is the root of the triad expressed as an integer (mod 12), and σ is a sign representing its mode (+ for major, - for minor).

Example 6.2. $\Delta = (0, +)$ represents a C major triad and $\Delta = (6, -)$ represents an f# minor triad.

Theorem 6.3. The set of all 24 major and minor triads, forms a abelian group with multiplication defined by

$$(t_1, \delta_1)(t_2, \delta_2) = (t_1 + t_2, \delta_1\delta_2)$$

We call this set Γ .

Proof. This group is clearly isomorphic to $\mathbb{Z}_{12} \times \mathbb{Z}_2$, which by Theorem 2.23 is a group.

Definition 6.4. Given $\Delta_1 = (r_1, \delta_1)$ and $\Delta_2 = (r_2, \delta_2)$, the transposition level $t = r_2 - r_1$ is the interval between the roots and the sign factor $\delta = \delta_1\delta_2$ is the change in sign. (δ is multiplied as expected with $++ = +, +- = -, -+ = -$ and $-- = +$.) The Γ -interval $\text{int}(\Delta_1, \Delta_2)$ is the ordered pair (t, δ) where t and δ are the transposition level and sign factor as defined above.

Example 6.5. The Γ -interval from $(0, +)$ (C major) to $(6, -)$ (f# minor) is $(6, -)$.

6.1. Introduction to Triadic Transformations

Definition 6.6. A triadic transformation is a bijective mapping from Γ to itself. In other words, it is a permutation of Γ .

Theorem 6.7. The set of all triadic transformations forms a group G . Proof. After numbering the triads, this group is clearly isomorphic to S_{24} .

The order of G is huge: 24 factorial. However, most of these transformations have little musical meaning since the action of a transformation on one triad may not resemble its action on another triad.

6.2. V, the Uniform Triadic Transformations

Of particular musical interest are the UTTs because they operate on all major triads in the same manner. Similarly, the UTTs have one action for all minor triads.

Definition 6.8. Consider the triadic transformation that transforms (r, σ) to (r', σ') . It is a uniform triadic transformation (UTT) if it transforms $(r + t, \sigma)$ to $(r' + t, \sigma')$ $\forall t \in \mathbb{Z}_{12}$.

It is important to note that not all musically interesting transformations are UTTs. The inversions TnI , for example, are not part of the UTTs.

Any UTT is completely determined by three parameters:

- t^+ , its transposition level for a major triad
- t^- , its transposition level for a minor triad
- σ , its sign. (Note: it may seem that σ could be different for major and minor triads. However, in order to be a transformation, a UTT must map Γ to itself. Thus, if it switches major triads to minor, it must switch minor triads to major. That is $\delta^+ = -\delta^-$. Positive σ implies no change in mode (it is **mode-preserving**), negative σ implies switching to the opposite mode (it is **mode-reversing**).)

We can thus denote any UTT U by the ordered triple $U = \langle \sigma, t^+, t^- \rangle$. Example 6.9. We will convert Riemann's P , L and R in UTT notation:

$$P = \langle -, 0, 0 \rangle \quad L = \langle -, 4, 8 \rangle \quad R = \langle -, 9, 3 \rangle$$

Note, Hook uses left-to-right orthography. Thus, $U_1 U_2$ implies “first U_1 then U_2 .” As usual, $U_2 = U U_1$, etc. Although it is less intuitive for mathematicians, we will adhere to his notation.

6.2.1 Multiplication on V

Multiplication on V should clearly be composition. Before we derive a general formula for the composition of two UTTs, let us consider some concrete examples.

Example 6.10. Consider the UTTs $U = \langle +, 4, 7 \rangle$ and $V = \langle -, 5, 10 \rangle$. Let us calculate the product $UV = \langle \delta_{UV}, t_{UV}^+, t_{UV}^- \rangle$. When UV acts on a CM triad ($\Delta = (0, +)$) we have:

$$(0, +) \xrightarrow{U} (4, +) \xrightarrow{V} (9, -)$$

Thus, UV transforms the major triads through the Γ -interval (9, -). We can deduce that $\delta_{UV} = -$ and $t_{UV}^+ = 9$.

When UV acts on a cm triad ($\Delta = (0, -)$) we have:

$$(0, -) \xrightarrow{U} (7, -) \xrightarrow{V} (5, +)$$

Thus, UV transforms the minor triads through the Γ -interval (5, +) and $t_{UV}^- = 5$. Hence, $UV = \langle -, 9, 5 \rangle$

This product may be calculated by multiplying the signs ($\delta_{UV} = \delta_U \delta_V$) and adding the corresponding transposition levels ($t_{UV}^+ = t_U^+ + t_V^+$; $t_{UV}^- = t_U^- + t_V^-$). Figure 6 depicts a visual representation of UV.

Example 6.11. Now consider the product VU. In this case we have

$$(0, +) \xrightarrow{V} (5, -) \xrightarrow{U} (0, -)$$

and

$$(0, -) \xrightarrow{V} (10, +) \xrightarrow{U} (2, +)$$

Therefore, $VU = \langle -, 0, 2 \rangle$. In this case, the signs were multiplied as before, the transposition levels were “cross-added.” That is, $t_{UV}^+ = t_U^+ + t_V^-$ and $t_{UV}^- = t_V^+ + t_U^-$.

We can see that in the above example, the “cross-adding” was due to the sign of the first transformation. In the first case, the first UTT (U) was mode-preserving, so the second UTT (V) acted on the same mode as U. Thus, the corresponding transposition levels were applied in succession. In the second case, the first UTT (V) was mode-reversing, so the second UTT (U) acted on the opposite mode as V and opposite transposition levels were combined. This leads us to the general form of UTT multiplication:

Theorem 6.12. Consider two UTTs $U = \langle \delta_U, t_U^+, t_U^- \rangle$ and $V = \langle \delta_V, t_V^+, t_V^- \rangle$. Multiplication on V is given by $UV = \langle \delta_U \delta_V, t_U^+ + t_V^{(\delta_U)}, t_U^- + t_V^{(-\delta_U)} \rangle$

The reader can verify that following the process above using two arbitrary elements in V will give the desired result.

6.2.2 Inversion on V

Again, before we derive a general formula for the inverse of a UTT, let us consider some concrete examples.

Example 6.13. Consider the UTT $U = \langle +, 4, 7 \rangle$. Because $(0, +) \xrightarrow{U} (4, +)$ and $(0, -) \xrightarrow{U} (7, -)$, we need $(4, +) \xrightarrow{U^{-1}} (0, +)$ and $(7, -) \xrightarrow{U^{-1}} (0, -)$. Thus, $U^{-1} = \langle +, 8, 5 \rangle$. Note how this is simply the inversion of the transposition levels: $\langle +, -4 \pmod{12}, -7 \pmod{12} \rangle$.

Example 6.14. Now consider the UTT $V = \langle -, 5, 10 \rangle$. $(0, +) \xrightarrow{V} (5, -)$ and $(0, -) \xrightarrow{V} (10, +)$. Thus, $(5, -) \xrightarrow{V^{-1}} (0, +)$ and $(10, +) \xrightarrow{V^{-1}} (0, -)$. Therefore, $V^{-1} = \langle -2, 7 \rangle$ or $\langle -, -10 \pmod{12}, -5 \pmod{12} \rangle$. In this case, the transposition levels are not only inverted, but interchanged. Once again, this is due to the sign of V .

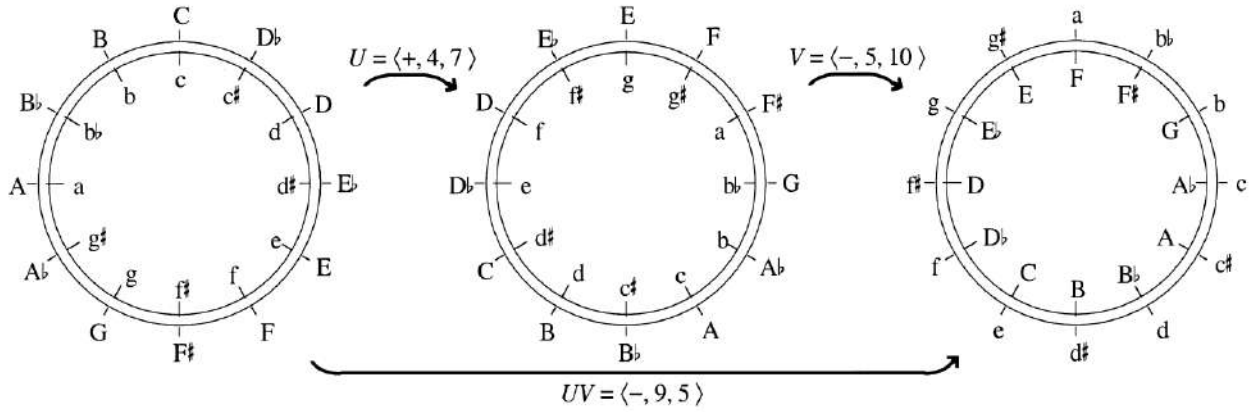


Figure 7: Visual representation of the UTT equation $\langle +, 4, 7 \rangle \langle -, 5, 10 \rangle = \langle -, 9, 5 \rangle$

Theorem 6.16. The set V of UTTs is a group that is isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$

Proof. Remember from Section 2.4.3 how we represented $G \times G$ in the form $r_1^m r_2^n$. Let G be \mathbb{Z}_{12} and let us switch the 1 and 2 to + and -. Then the elements of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ are $s r_+^m r_-^n$ where $m, n \in \mathbb{Z}_{12}$.

Also note that the transpositions, which are equivalent to the transposition levels of a UTT, are isomorphic to the rotations of the D_{12} by $T_n \rightarrow r^n$. We initially wrote that the $T_n/T_n I$ group was isomorphic by $T_n \rightarrow r^{12-n}$. This reflected our visual representation of the two groups. However, the groups are still isomorphic if we choose $T_n \rightarrow r^n$, which makes the following argument clearer.

It seems likely that the UTTs are isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ by $\langle \sigma, t^+, t^- \rangle \rightarrow s r_+^m r_-^n$. We have already shown that the UTTs have multiplication and inverses. We only need to show that it follows the multiplication of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$. That is, $(r_+^m r_-^n)s = s(r_-^n r_+^m)$.

$$\begin{aligned}
 (r_+^m r_-^n)s &= (e r_+^m r_-^n)(see) \\
 &= \langle -, 0, 0 \rangle \langle +, t_m^+, t_n^- \rangle \\
 &= \langle -, 0 + t_n^-, 0 + t_m^+ \rangle \\
 &= \langle -, t_n^-, t_m^+ \rangle \\
 &= s(r_-^n, r_+^m)
 \end{aligned}$$

Thus, multiplication is preserved and the isomorphism holds.

6.2.3 Even and Odd UTTs

UTTs can be classified as “even” or “odd” in multiple ways. Let us begin with “even/odd in the sense of total transposition.”

Definition 6.17. We say that a UTT $U = \langle \sigma, t^+, t^- \rangle$ is even (or, more fully, even in the sense of total transposition) if its total transposition $\tau(U) = t^+ + t^-$ is an even number. U is odd (in the sense of total transposition) if $\tau(U)$ is an odd number.

Definition 6.19. A UTTs is even (in the sense of permutation theory) if it can be written as a product of an even number of 2-cycles and odd (in the sense of permutation theory) if it can be written as a product of an odd number of 2-cycles.

It is remarkable that the two definitions of even or odd (in the sense of total transposition versus permutation theory) are actually equivalent.

Theorem 6.20. A UTT is even in the sense of total transposition if and only if it is even in the sense of permutation theory.

6.3. \mathbb{R} , the Riemannian UTTs

Recall the Neo-Riemannian operators P , L and R as introduced in Section 5 and written as UTTs in Example 6.9. For each, the transposition level for a major triad is equal and opposite that of a minor triad. We define the Riemannian UTTs as follows.

Definition 6.21. A Riemannian UTT is a UTT such that $t^+ = -t^-$.

Theorem 6.22. The set of \mathbb{R} of Riemannian UTTs is isomorphic to D_{12} .

Proof. D_{12} can be defined as the group of order 24 generated by s and r , such that $s^2 = e$, $r^{12} = e$ and $sr = r^{-1}s$

The generators of \mathbb{R} are $\langle -, 0, 0 \rangle$ and $\langle +, 1, 11 \rangle$.

$$(\langle -, 0, 0 \rangle)^2 = \langle -, 0+0, 0+0 \rangle = \langle +, 0, 0 \rangle = e \in \mathbb{R}$$

$$(\langle +, 1, 11 \rangle)^{12} = \langle +, 12 \cdot (1), 12 \cdot (11) \rangle = \langle +, 0, 0 \rangle = e$$

$$(\langle +, 1, 11 \rangle)^{-1} = \langle +, 11, 1 \rangle$$

$$\langle -, 0, 0 \rangle \langle +, 1, 11 \rangle = \langle -, 0 + 11, 0 + 1 \rangle = \langle -, 11 + 0, 1 + 0 \rangle$$

$$= \langle +, 1, 11 \rangle \langle -, 0, 0 \rangle = r^{-1}s$$

6.4 \mathbb{K} , the Subgroups of \mathbb{V}

Generally, it is difficult to list all the subgroups of a given group G . However, it is possible to list all the subgroups of \mathbb{V} .

Definition 6.23. Give two integers a and b (mod 12), we define three subsets of \mathbb{V} as follows.

- $K^+(a)$ is the set of all mode-preserving UTTs of the form $\langle +, n, an \rangle$ as n ranges through the integers mod 12.

- $K^-(a, b)$ is the set of all mode-reversing UTTs of the form $\langle -, n, an+b \rangle$.
- $K(a, b) = K^+(a) \cup K^-(a, b)$

Theorem 6.24. $K(a, b)$ is a subgroup of V if and only if the numbers a and b satisfy $a^2=1$ and $ab = b \pmod{12}$.

The condition $a^2 = 1$ is satisfied only for $a = 1, 5, 7$ and 11 . If $a = 1$ then the condition $ab = b$ is automatically satisfied. For other values of a , the allowable values of b are different in each case. The following is a complete list of the groups $K(a, b)$:

$K(1,0), K(1,1), K(1,2), \dots, K(1,11)$
 $K(5, 0), K(5, 3), K(5, 6), K(5, 9)$
 $K(7, 0), K(7, 2), K(7, 4), K(7, 6), K(7, 8), K(7, 10) K(11, 0), K(11, 6)$

7. Musical Application

The UTTs of order 24 are of considerable musical interest. When such a transformation is applied repeatedly, the resulting chain of triads will cycle through all 24 major and minor triads before returning to the original one. Take, for example, the UTT $U = \langle -, 9, 8 \rangle$. Its repeated application produces a chain in the scherzo of Beethoven's Ninth Symphony :

$$C \xrightarrow{U} a \xrightarrow{U} F \xrightarrow{U} d \rightarrow \dots \xrightarrow{U} A$$

This chain is 19 triads long, only five short of a complete cycle.

Such triad chains are rarely prolonged to this extent. There are, however, examples from literature that circumnavigate the entire cycle of 24 triads. These are found in collections of pieces such as Bach's Well-Tempered Clavier and the Chopin Preludes.

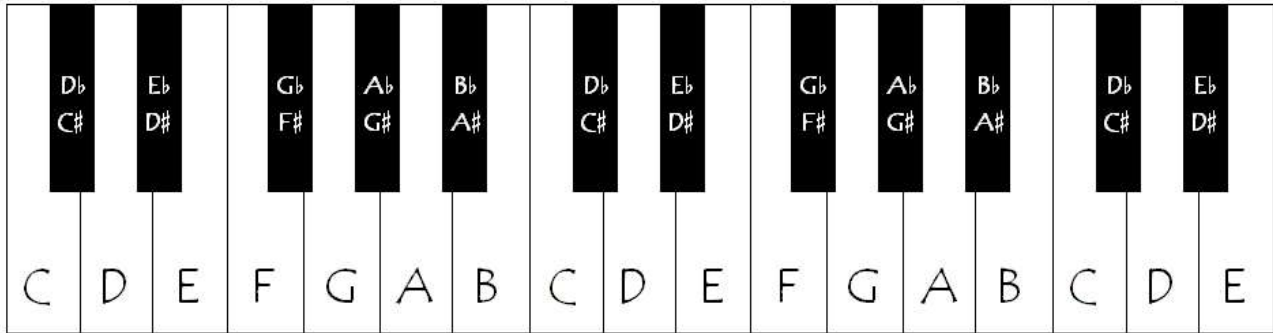


Figure 8: A piano with the keys labeled

8. Conclusion

We can see that Hook's UTTs not only have interesting mathematical properties, but also musical significance. Musically, the choice of triads is non-arbitrary since triads occur throughout music. Mathematically, however, the set choice is arbitrary. Some current research in music theory investigates the generalization Hook's UTTs to larger chords or even to pitch-class sets. The flexibility these generalisations will provide may greatly improve atonal analysis.

References

- [1] Armstrong, M. Groups and Symmetry. Springer-Verlag, 1988.
- [2] Dummit, D. S., and Foote, R. M. Abstract Algebra, third ed. Wiley, 2003.
- [3] Hook, J. Uniform triadic transformations. *Journal of Music Theory* 46, 1-2 (2002), 57–126.
- [4] Straus, J. N. Introduction to Post-Tonal Theory, second ed. Prentice-Hall, Inc., 2000.

***RAMAKRISHNA MISSION VIVEKANANDA CENTENARY
COLLEGE***

- **Name: Sanjay Karmakar**
- **Reg no: A01-1152-113-025-2019**
- **Roll: 2022151111**
- **College roll: 338**
- **Topic: Cayley's theorem by group homomorphism and
Group action**
- **Supervised by: Prof. Pravanjan Kumar Rana**

ACKNOWLEDGEMENT

We would like to express my special thanks of gratitude to our group theory teacher “Mr. Pravanjan Kumar Rana” for his able guidance and support in completing this project.

I would also like to extend my gratitude to principal “swami Kamalasthanada maharaj” for providing me with all facility that was required.

Date:

15-01-2022

Amit Kumar Ghosh (2022151113)

Sanjay Karmakar (2022151111)

Souvik Pal (2022151118)

■ **CONTENTS:**

- **Definition of group action**
- **Definition of group homomorphism**
- **Induced homomorphism**
- **Cayley's theorem**
- **Proof by Cayley's theorem**
(by group homomorphism method)
(by group action method)

TOPIC: CAYLEY'S THEOREM BY GROUP HOMOMORPHISM AND GROUP ACTION

Definition of Group Action:

Let G be a group and X be a set. Then G is said to act on X if there is a mapping $\phi: G \times X \rightarrow X$, with $\phi(a, x)$ written $a * x$ such that for all $a, b \in G, x \in X$

- $a * (b * x) = ab * x$
- $e * x = x$

The mapping ϕ is called **the action of G on X** , and X is said to be a G -set.

Definition of Group homomorphism:

Let $(G, *)$ and (G', \circ) be two groups and f be a function from G into G' . Then f is called a **group homomorphism** of G to G' if for all $a, b \in G$,

$$f(a * b) = f(a) \circ f(b)$$

Theorem:

Let G be a group and let X be a set.

- If X is a G -set, then the action of G on X induces a homomorphism $\phi: G \rightarrow S_X$.
- Any homomorphism $\phi: G \rightarrow S_X$ induces an action of G onto X .

Proof:

At first we define $\phi: G \rightarrow S_X$ by $(\phi(a))(x) = ax$, $a \in G, x \in X$

Now we have to prove $\phi(a) \in S_X$

Let $x_1, x_2 \in X$

Then,

$$(\phi(a))(x_1) = (\phi(a))(x_2)$$

$$\Rightarrow ax_1 = ax_2$$

$$\Rightarrow x_1 = x_2$$

$\therefore \phi(a)$ is one-one.

Now,

$$\begin{aligned} x_2 &= a(a^{-1}x_2) \\ &= (\phi(a))(a^{-1}x_2) \quad , a^{-1}x_2 \in X \end{aligned}$$

Thus, $\phi(a) \in S_X$

Now, let, $a, b \in G$

Then

$$\begin{aligned} \phi(ab)(x) &= (ab)(x) \\ &= a(bx) \\ &= a(\phi(b)(x)) \\ &= \phi(a)\phi(b)(x) \quad , \forall x \in X \end{aligned}$$

Here, $\phi(ab) = \phi(a)\phi(b)$

So, ϕ is a homomorphism.

Now we define,

$$a * x = \phi(a)(x)$$

That is $ax = (\phi(a))(x)$

Let, $a, b \in G$

Then

$$\begin{aligned}
(ab)(x) &= (\phi(ab))(x) \\
&= (\phi(a)\phi(b))(x) \\
&= \phi(a)(\phi(b)(x)) \\
&= \phi(a)(bx) \\
&= a(bx)
\end{aligned}$$

Also $ex = (\phi(e))(x) = e$ (where e is the identity element)

Hence X is a G -set.

Application: Cayley's Theorem:

Let G be a group. Then G is isomorphic to a subgroup of group S_G .

Proof by group action method:

Here we want to prove this theorem by the group action method.

G is a G -set.

Where G acts on G by group operation.

This left action induces a homomorphism $\phi: G \rightarrow S_G$

Where $(\phi(a))(x) = ax \quad a \in G, x \in G$

$$\begin{aligned}
\text{Ker } \phi &= \{a \in G : \phi(a) = \text{identity permutation on } G\} \\
&= \{a \in G : ax = x, \forall x \in G\} \\
&= \{e\}
\end{aligned}$$

Hence ϕ is a monomorphism.

Now by first isomorphism theorem $\frac{G}{\text{ker } \phi} \cong \text{subgroup of } S_G$

So, the theorem is proved.

Proof by group homomorphism method:

Here we want to prove this theorem by the homomorphism method.

Let G be a group.

For any $a \in G$ the mapping $f_a : G \rightarrow G$, given by $f_a(x) = ax$ for all $x \in G$ is a bijection, because,

$$\begin{aligned} ax &= ax' \\ \Rightarrow x &= x' \end{aligned}$$

And $y = f_a(a^{-1}y)$ for all $x, x', y \in G$

Considering the mapping, $\phi : G \rightarrow S_G$

Where $\phi(a) = f_a$ for all $a \in G$

Where S_G is a symmetric group on the set G

Now, for all $a, b, x \in G$,

$$\begin{aligned} f_{ab}(x) &= abx \\ &= f_a(bx) \\ &= f_a(f_b(x)) \\ &= (f_a f_b)(x) \end{aligned}$$

Hence $\phi(ab) = \phi(a)\phi(b)$

Therefore, ϕ is a homomorphism.

And $\text{Im } \phi$ is a subgroup of S_G

Moreover,

$$\begin{aligned} \phi(a) &= \phi(b) \\ \Rightarrow ax &= bx \quad \forall x \in G \\ \Rightarrow a &= b \end{aligned}$$

Hence ϕ is an injective homomorphism.

Therefore G is isomorphic to a subgroup of S_G

The above isomorphism is called the **left regular representation** of G .

Similarly, we have a right regular representation.

Reference:

To write this project, we take help of these following books,

- Abstract Algebra (Dummit, David, Foote)
- Contemporary abstract algebra (Joseph Gallian)
- Fundamentals of Abstract Algebra (Malik, Moderesen, Sen)

College Name: Ramakrishna Mission Vivekananda Centenary College

Name: Partha Das

Reg. No: A01-1152-113-030-2019

Exam Roll No: 2022151114

College Roll No: 345

Project Topic: Todd-Coxeter Algorithm

Supervised by: Pravanjan Kumar Rana

Acknowledgement

I would like to express my special thanks of gratitude to my advisor, Prof. Pravanjan Kumar Rana, who introduced me to the wonderful project work. I would also like to thank him for the guidance, patience, and help and for contributing from his abundance experience, knowledge and wisdom. It was an honour for me to get a glimpse to his world and way of thinking. My friends Anischay Pal and Sreyan Jha also helped me to do this project work, I am also thankful to them.

CONTENT

<u>SI No.</u>	<u>Subject</u>	<u>Page No.</u>
01.	Introduction	4
02.	Todd-Coxeter Algorithm	4-6
03.	Example	7-13
04.	Implementation	13-15
05.	Application	15-16
06.	Conclusion	17
07.	References	17

Introduction:

In group theory, the **Todd–Coxeter algorithm**, created by J. A. Todd and H. S. M. Coxeter in 1936, is an algorithm for solving the coset enumeration problem. Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm is a strategy for writing down the set of left cosets of H in G together with the action of G on the set.

Todd–Coxeter Algorithm:

Let G be the finitely presented group

$$G := \langle g_1, g_2, \dots, g_n \mid r_1(g_1, g_1, g_2, \dots, g_n) = e, \dots, r_m(g_1, g_1, g_2, \dots, g_n) = e \rangle$$

or shorter $G := \langle E \mid R \rangle$ where $E := \{g_1, g_2, \dots, g_n\}$ and $R := \{r_i(g_1, g_1, g_2, \dots, g_n) \mid i = 1, 2, \dots, m\}$ where each relator $r_i(g_1, g_1, g_2, \dots, g_n)$ is a word in g_1, g_2, \dots, g_n and e is the identity of G , and let H be the subgroup of G generated by the set S of words,

$$S := \{s_1(g_1, g_1, g_2, \dots, g_n), \dots, s_p(g_1, g_1, g_2, \dots, g_n)\}$$

that is, $H := \langle S \rangle$.

The algorithm is based on two simple facts:

1. If $s \in S$, then $Hs = H$.
2. If $r(g_1, \dots, g_n)$ is a relator, then for any coset Hx , $x \in G$ we have $Hxr(g_1, \dots, g_n) = Hx$. So if $r(g_1, \dots, g_n) = g_{i1} \dots g_{it}$ where each g_{ij} is a generator or an

inverse of a generator, then: $H_0 := Hx$, $H_1 := H_{0g_{i1}}$, $H_2 := H_{1g_{i2}}$, \dots , $H_j := H_{j-1g_{ij}}$ is defined, then $H_t = H_0$.

Now, for the procedure itself: for each word that generates the subgroup H we maintain a one-line table, called a subgroup table. The row is labelled as 1 for the coset H itself. The columns are labelled by the factors of the generator of the word. That is, if $s_j = g_{i1} \dots g_{ik}$ is a generator of H , then we have $k + 1$ columns.

Subgroup Table

g_{i1}	g_{i2}	\dots	g_{ik}
1			1

If we look at the table as a matrix of order $1 \times (k + 1)$, then the entry $(1, g_{ij})$ in the table, if defined, is the number of the coset we get from the multiplication $1 \cdot g_{i1} \dots g_{ij}$.

For each relator, $r(g_1, \dots, g_n)$ we have a relation table. Relation tables will give us information in case two cosets which have numbered differently are the same. If a relation acts on two cosets in exactly the same way, then these cosets must be identical. The rows of the relation tables are labelled with the numbering we defined for the cosets. Similarly to the subgroup table, given a relator $r_i = g_{i1} \dots g_{ik}$, we have $k + 1$ columns.

Relation table for $r_i = g_{i1} \dots g_{ik}$

g_{i1}	g_{i1}	\dots	g_{ik}
1			1
2			2
.			.
.			.
.			.
t			t
.			.
.			.

As in the subgroup table, the entry (n, g_{ij}) if defined, is the coset we get from the multiplication $n \cdot g_{i1} \cdot g_{i2} \cdots g_{ij}$. Since we know that $r_i = g_{i1} \cdots g_{ik} = e$, we get that $Hxr_i = Hx$. So the entry (n, g_{ik}) is n .

Finally, we would like to have a table that keeps track for us on the result of multiplications. This table is the coset table. The rows will be labelled with the numbers of the cosets, and the columns will be labelled by the generators of G and their inverses (unless a generator is an involution). The entry (n, g_i) , if defined, is $n \cdot g_i$ for the coset n and the generator g_i .

When the last entry in a row of a relation table or a subgroup table is filled in, we get an extra piece of information, in the form of $n \cdot g = l$, for some cosets n, l and a generator g . This extra piece of information is called a deduction. When getting a deduction we can face three situations:

- (i) The entries (n, g) and (l, g^{-1}) are still empty. In this case, we just fill the number l in the entry (n, g) and the number n in the entry (l, g^{-1}) . We also insert this information into all other relevant places in the other tables.
- (ii) The entry (n, g) is already filled with the number l . In this case, the deduction brings no new information.
- (iii) At least one of the entries (n, g) or (l, g^{-1}) in the coset tables is filled with a number different from l or n , respectively. In this case, we conclude that we have two different numbers to the same coset. This phenomenon is called a coincidence. When a coincidence is found, we replace both numbers by the smaller one in all places they occur.

The process terminates when all the entries of the coset, relation and subgroup tables are filled.

We would like to give a detailed example of the Todd-Coxeter Algorithm for the group S_4 , using generators and relations, as follows:

$G := \langle a, b, c \mid a^2 = b^2 = c^2 = e, (ab)^3 = e, (bc)^3 = e, (ac)^2 = e \rangle$
and taking the subgroup

$$H := \langle a, b \rangle.$$

We have to use some useful proposition

- (i) The set of transpositions $\{(1, k) \mid 1 \leq k \leq n\}$ generate S_n , for $n \geq 2$
- (ii) The set of transpositions $\{(12), (23), \dots, (n-1, n)\}$ generate S_n , for $n \geq 2$.

First, we define three cosets and try to fill in the tables. Then we will be able to see whether we need to define more cosets in order to complete the tables, or not.

We define:

$$1 := H, 2 := 1c, 3 := 2b.$$

The subgroup tables are already closed, and as expected, we did not gain any additional information from them.

Subgroup Tables

<u>a</u>		<u>b</u>	
1	1	1	1

However, from the definitions and the relations in the group G , we can immediately derive the following: $2c = 1$, $3b = 2$, as b and c are of order 2. We should note that there are a few possible ways to fill in the tables. One can start from the left or from the right and then can continue using any combination of them. Nevertheless, eventually one arrives at the same result.

Now, let us start filling in the coset and relation tables:

Coset table

	a	b	c
1	1	1	2
2	2	3	1
3		2	3

Relation tables for $a^2 = e$, $b^2 = e$, $c^2 = e$

<u>a</u>		<u>b</u>		<u>c</u>	
1	1	1	1	1	2
2	2	2	3	2	1
3	3	3	2	3	3

Relation table for $(ab)^3 = e$

	<u>a</u>	<u>b</u>	<u>a</u>	<u>b</u>	<u>a</u>	<u>b</u>
1	1	1	1	1	1	1
2	2	3			3	2
3			3	2	2	3

Relation table for $(ac)^2 = e$

	a	c	a	c
1	1	<u>2</u>	<u>2</u>	1
2	2	1	1	2
3	3		3	3

Relation table for $(bc)^3 = e$

	b	c	b	c	b	c
1	1	2	3	3	2	1
2	<u>3</u>	<u>3</u>	2	1	1	2
3	2	1	1	2	3	3

In the process of filling in the tables we have received the following deductions, $2a = 2$, $3c = 3$, which we have underlined in the table, in the place we got them.

Now, one can define one more coset and continue, or to define a few more at once. As we shall see, it is enough to define only one more coset, namely, $4 := 3a$ to complete all the tables. However, since we would like to demonstrate the notion of "coincidences" we shall take the latter approach: we shall define three more cosets at once: $4 := 3a$, $5 := 4b$, $6 := 4c$. Continuing filling in the tables gives

	a	b	a	b	a	b
1	1	1	1	1	1	1
2	2	3	<u>4*</u>	<u>4*</u>	3	2
3	4	<u>5*</u>	<u>3*</u>	2	2	3
4	3	2	2	3	5	4
5	3	2	2	3	4	5
6	3	2	2	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 ₅	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we receive the following deductions: $4b = 4$ and $5a = 3$. However, as we see in the coset table, the place of $4b$ is already filled with 5. Therefore, we get a coincidence: cosets 4 and 5 are the same coset of H in the group G . Similarly, the place of $3a$ is already filled with 4 in the coset table, which means, as have already discovered, that 4 and 5 are the same coset. We note that coincidences are marked in the tables with asterisk(*). Equipped with the previous information, let us continue to the other relation tables.

	a	c	a	c
1	1	2	2	1
2	2	1	1	2
3	4	<u>6*</u>	<u>3*</u>	3
4	3	3	4	4
5	3	3	4	5
6	3	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 _{5,6}	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we get the information that $6a = 3$ or, equivalently, $3a = 6$. This yields another coincidence: this time we get that cosets 4 and 6 are the same cosets of H in G . So, from the last two coincidences we have $4 = 5 = 6$. These coincidences yield full information about the multiplication of all the elements we have, or in other words, we filled in the whole coset table, and thus can fill in the rest of the tables completely. As we said in the description of the algorithm, we take the smallest integer in a coincidence to represent the equal cosets.

	a	b	c
1	1	1	2
2	2	3	1
3	$4_{5,6}$	2	3
4	3	5_4	6_4
5	3	4	4
6	3	4	4

	a			b			c	
1	1	1	1	1	1	1	2	1
2	2	2	2	3	2	2	1	2
3	4	3	3	2	3	3	3	3
4	3	4	4	5	4	4	6	4
5	3	5	5	4	5	5	4	5
6	3	6	6	4	6	6	4	6

	b	c	b	c	b	c
1	1	2	3	3	2	1
2	3	3	2	1	1	2
3	2	1	1	2	3	3
4	4	4	4	4	4	4
5	4	4	4	4	4	5
6	4	4	4	4	4	6

Eventually, we receive four different cosets of H in G , which are 1,2,3 and 4. This means that $[G : H] = 4$, and since $|H| \leq 6$ then we get an upper bound to the order of G , that is, $|G| \leq 24$. On the other hand, we know that the three transpositions (12),(23),(34), of which the generators of G act on the cosets 1,2,3 and 4, generate S_4 and we get an epimorphism from G onto S_4 (or equivalently, S_4 is a homomorphic image of G), which means that $|G| \geq 24$. All in all, we get that $|G| = 24$ and thus $G \cong S_4$.

Implementation

Now we give a concrete implementation of the algorithm in Python. For simplicity, we will just compute $S_3/\langle b \rangle$ with the presentation $\langle a, b | a^3, b^2, abab \rangle$

The main data structures are

```
idents = []

neighbors = []
to_visit = 0

ngens = 2
rels = [
    (1, 0), # a^-1a
    (3, 2), # b^-1b
    (0, 0, 0), # a^3
    (2, 2), # b^2
    (0, 2, 0, 2) # abab
]
hgens = [
    (2,), # b
]

def find(c):
    c2 = idents[c]
    if c == c2:
        return c
    else:
        c2 = find(c2)
        idents[c] = c2
        return c2

def new():
```

```

c = len(idents)
idents.append(c)
neighbors.append((2*ngens)*[None])
return c

def unify(c1, c2):
    c1 = find(c1)
    c2 = find(c2)
    if c1 == c2:
        return
    c1, c2 = min(c1, c2), max(c1, c2)
    idents[c2] = c1
    for d in range(2*ngens):
        n1 = neighbors[c1][d]
        n2 = neighbors[c2][d]
        if n1 == None:
            neighbors[c1][d] = n2
        elif n2 != None:
            unify(n1, n2)

def follow(c, d):
    c = find(c)
    ns = neighbors[c]
    if ns[d] == None:
        ns[d] = new()
    return find(ns[d])

def followp(c, ds):
    c = find(c)
    for d in reversed(ds):
        c = follow(c, d)
    return c

start = new()

for hgen in hgens:
    unify(followp(start, hgen), start)

while to_visit < len(idents):
    c = find(to_visit)
    if c == to_visit:
        for rel in rels:
            unify(followp(c, rel), c)
    to_visit += 1

print ("done")

cosets = [c for i, c in enumerate(idents) if i == c]

```

```
perms = [[cosets.index(follow(c, 2*d)) for i, c in enumerate(cosets)]
          for d in range(ngens)]

def cycle(perm):
    parts = []
    for i in range(len(perm)):
        part = [str(i+1)]
        k = perm[i]
        while k != i:
            if k < i: break
            part.append(str(k+1))
            k = perm[k]
        else:
            parts.append(" ".join(part))
    return "("+" ".join(parts)+")"
for d in range(ngens):
    print ("g%d =" %d, cycle(perms[d]))
```

For these particular relations, the output is

```
done
g0 = (1 2 3)
g1 = (1) (2 3)
```

Application:

By using this algorithm, Coxeter and Todd showed that certain systems of relations between generators of known groups are complete, that is constitute systems of defining relations. If the order of a group G is relatively small and the subgroup H is known to be uncomplicated, then the algorithm can be carried out by hand and gives a reasonable description of the group G . It is a systematic procedure for enumerating the cosets of a subgroup of finite index in a group given by generators and relations. The algorithm has been an important component in most

computer programs to date dealing with symbolic calculation in algebra.

We use programmes for the Todd-Coxeter coset enumeration algorithm and the modified Todd-Coxeter coset enumeration algorithm to investigate a class of generalised Fibonacci groups. In particular we use these techniques to discover a finite non-metacyclic Fibonacci group.

There are a number of things one can deduce from the result of the algorithm.

- Of course, if it terminates, we deduce $[G:H]$ is finite (and know what it equals).
- A permutation representation of G/H , given by a permutation of G/H for each generator of G .
- Whether H is a normal subgroup. This can be determined by seeing whether each generator's permutation is an element of $\text{Aut}(G/H)$, since then $\text{Aut}(G/H) = G/H$, implying H is normal.
- An algorithm for the word problem for the group. Given two words, follow the graph from the basepoint to see whether they end on the same vertex.
- The algorithm also helps to compute the data of a uniform polytope.

Conclusion:

The Todd–Coxeter algorithm can be applied to infinite groups and is known to terminate in a finite number of steps, provided that the index of H in G is finite. On the other hand, for a general pair consisting of a group presentation and a subgroup, its running time is not bounded by any computable function of the index of the subgroup and the size of the input data.

References:

- .Brown, Ken. *The Todd-Coxeter procedure*.
- Coxeter, H. S. M.; Moser, W. O. J. (1980). *Generators and Relations for Discrete Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 14 (4th ed.). Springer-Verlag 1980. ISBN 3-540-09212-9. MR 0562913.
- Seress, Ákos (1997). "An introduction to computational group theory" (PDF). Notices of the American Mathematical Society. 44 (6): 671–679. MR 1452069.

Pranay Mandal

Registration No : A01-1122-113-059-2018

Roll no : 1370

Semester : 5

Paper : CC-12

**Topic : The Framework of Music Theory as
Represented with Groups**

Acknowledgement

I would like to express my special thanks of gratitude to our beloved **Pravanjan Kumar Rana Sir** who gave me the opportunity to do this wonderful project on the topic **The Framework of Music Theory as Represented with Groups**, which also helped me in doing a lot of research and I come to know about so many new things.

Secondly I would like to thank my friends **Shubhajit Bhowmick** and **Satyabrata Pradhan** who helped me a lot in finishing this project within the limited. It helped me increase my knowledge and skills.

The Framework of Music Theory as Represented with Groups

Contents

- 1 Introduction
- 2 Basic Group Theory
 - 2.1 What is a group ?
 - 2.2 Permutations
 - 2.3 Morphisms
 - 2.3.1 Homomorphisms
 - 2.3.2 Isomorphisms
 - 2.3.3 Automorphisms
 - 2.4 Products
 - 2.4.1 Direct Products
 - 2.4.2 Semidirect Products
 - 2.4.3 Wreath Products
- 3 Music Theory
 - 3.1 Basic concepts of atonal music theory
 - 3.1.1 T_n , the Transpositions
 - 3.1.2 $T_n I$, the Inversions
- 4 Group Theory as a Structure for Atonal Music Theory
- 5 A Flaw in Atonal Music Theory
- 6 Uniform Triadic Transformations

6.1 Introduction to Triadic Transformations

6.2 V , the Uniform Triadic Transformations

6.2.1 Multiplication on V

6.2.2 Inversion on V

6.2.3 Isomorphism to $Z_{12} \wr Z_2$

6.2.4 Even and Odd UTTs

6.3 R , the Riemannian UTTs

6.4 K , the Subgroups of V

7 Musical Application

8 Conclusion

References

1. Introduction

In 2002, a music theorist by the name of Julian Hook published a paper in the Journal of Music Theory titled, “Uniform Triadic Transformations.” In this paper, Hook generalized some existing music theoretical concepts and greatly improved their notation. Hook’s UTTs formed a group with interesting algebraic properties.

This paper will first give the reader a review of all necessary group theory to understand the discussion of Hook’s UTTs. Then it will review music theory (atonal theory in particular) and its evolution to the UTTs. Finally, it will discuss the UTTs themselves and conclude with some musical applications.

2 . Basic Group Theory

Group theory is a branch of mathematics that studies groups. This algebraic structure forms the basis for abstract algebra, which studies other structures such as rings, fields, modules, vector spaces and algebras. These can all be classified as groups with addition operations and axioms.

This section provides a quick and basic review of group theory, which will serve as the basis for discussions in the group theoretical structure as applied to music theory.

2.1 . What is a group?

A group is a set such that any two elements x and y can be combined via “multiplication” to form a unique product xy that also lies in the set. This multiplication is defined for every group and does not necessarily refer to the traditional meaning of “multiplication.” We now state the formal definition of a group:

Definition 2.1. A group is a set G together with a multiplication on G which satisfies three axioms:

- (a) The multiplication is associative, that is to say $(xy)z = x(yz)$ for any three (not necessarily distinct) elements in G .
- (b) There is an element $e \in G$, called an identity element, such that $xe = e = ex, \forall x \in G$
- (c) Each element $x \in G$ has an inverse x^{-1} which belongs to the set G and satisfies $x^{-1}x = e = xx^{-1}$

Theorem 2.2. Every group G satisfies the following properties:

- (a) The identity element e of G is unique
- (b) $\forall x \in G$, the inverse x^{-1} is unique

Note how commutativity of the multiplication is not required within a group. Therefore, we define an abelian group as follows:

Definition 2.3. A group G is abelian if its multiplication is commutative. That is, $xy = yx$ for any two elements in G .

To better illustrate the concept of a group, we now give some examples. Example 2.4. The reals excluding 0, $\mathbb{R} \setminus \{0\}$ under multiplication:

- The group is closed under multiplication: $\forall x, y \in \mathbb{R}, x \cdot y \in \mathbb{R}$

- The multiplication is associative: $\forall x, y, z \in \mathbb{R}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- The identity is 1: $\forall x \in \mathbb{R}, 1 \cdot x = x \cdot 1$
- The inverse of x is $\frac{1}{x}$: $\frac{1}{x} \cdot x = 1 = x \cdot \frac{1}{x}$

This group is abelian since $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$. Note how we must exclude 0 for this to be a group since there exists no inverse for 0. That is, there does not exist some $x \in \mathbb{R}$ such that $x \cdot 0 = 1$

Example 2.4. The integers $\mathbb{Z} \pmod{12}$, which we will denote as \mathbb{Z}_{12} , under addition $\pmod{12}$. (Note: in abstract algebra, $\mathbb{Z} \pmod{12}$ is generally notated as $\mathbb{Z}/(12)$ and \mathbb{Z}_{12} refers to another algebraic structure. However, in music theory, only $\mathbb{Z} \pmod{12}$ is of significance and we will use this more concise notation.)

- The group is closed under addition $\pmod{12}$: for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y \in \mathbb{Z}_{12}$.
- Addition $\pmod{12}$ is associative.
- The identity is 0.
- The inverse of x is $12-x$.

This group is also abelian since for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y = y +_{12} x$.

Example 2.6. The dihedral groups represent the symmetries of a regular polygon that map it onto itself. Consider the regular hexagon. Let r denote the rotation of through $\pi/3$ about the axis of symmetry perpendicular to the hexagon (rotating), let s denote the rotation through π about an axis of symmetry that lies in the plane of the plate (flipping), and let e denote the identity (leaving the hexagon unchanged). Then the dihedral group D_6 consists of the following 12 elements.

It may seem that the group is not closed under multiplication since the element sr is missing from the group. However, a rotation r takes the hexagon. A subsequent flip s takes the hexagon. Thus, rs is equivalent to r^5s . The reader can check that the whole group is indeed closed under multiplication. In general,

$$sr^n = r^{6-n}s, \forall n \in \mathbb{Z}_6$$

for the D_6 dihedral group.

Definition 2.7. The order of a group is the number of elements in the group.

Definition 2.8. The order of some element x of a group G is the smallest positive integer n such that $x^n = e$.

Definition 2.9. A subgroup of a group G is a subset of G which itself forms a group under the multiplication of G

Definition 2.10. A group G is cyclic if there exists an $x \in G$ such that for all $y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$. We call x a generator of G .

Definition 2.11. A permutation of an arbitrary set X is a bijection from X to itself.

Permutations can be denoted in multiple ways. Consider r from the D_6 dihedral group. We can represent it as a permutation of integers like so: (054321) , where each integer is sent to the one following it, and the final one is sent to the first. Likewise, we can write sr as $(01)(25)(34)$.

Definition 2.12. A permutation of the form $(a_1 a_2 \dots a_k)$ is called a cyclic permutation. A cyclic permutation of length k is called a k -cycle.

Definition 2.13. A transposition is 2-cycle. Any k -cycle $(a_1 a_2 \dots a_k)$ can be written as a product of transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$$

Note that transpositions may be written as many different products. This product is not unique, but is meant to show the existence of a product consisting only of transpositions.

Definition 2.14. An even permutation is a permutation that can be written as an even number of transpositions. The others are called odd permutations.

It may bother the reader that the a permutation in the form of a product of transpositions is not unique. Perhaps a permutation could be written as both an even number of transpositions and an odd number. However, the following theorem shows that the definition is well defined.

Theorem 2.15. Although any permutation can be written as a product of transpositions in infinitely many different ways, the number of transpositions which occur is always even or always odd.

Theorem 2.16. Consider the set X of n elements. The set of all permutations of X forms a group S_n called the symmetric group of degree n . Multiplication on this group is defined by composition of functions.

2.3 Morphisms

2.3.1 Homomorphisms

Definition 2.17. Let G and G' be groups. A homomorphism is a function $\phi : G \rightarrow G'$ that preserves the multiplication of G . Therefore, $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$

Example 2.18. Let ϕ be a function from D_{12} to Z_2 defined by $\psi(r^n) = 0$ and $\psi(r^n s) = 1$. Consider two elements x and y in D_{12} . We have four cases:

$$\bullet x = r^m, y = r^n;$$

$$\psi(xy) = \psi(r^m r^n) = \psi(r^{m+n}) = 0 = 0 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n;$$

$$\psi(xy) = \psi(r^m s r^n) = \psi(r^{m-n} s) = 1 = 1 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m, y = r^n s;$$

$$\psi(xy) = \psi(r^m r^n s) = \psi(r^{m+n} s) = 1 = 0 + 1 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n s;$$

$$\psi(xy) = \psi(r^m s r^n s) = \psi(r^{m-n} ss) = \psi(r^{m-n}) = 0 = 1 + 1 = \psi(x)\psi(y)$$

Hence, ϕ satisfies the properties of a homomorphism.

2.3.2 Isomorphisms

Definition 2.19. An isomorphism is a bijective homomorphism.

Example 2.20. \mathbb{Z}_{12} is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$. Consider the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$(0,0) \quad (0,1) \quad (0,2) \quad (0,3)$$

$$(1,0) \quad (1,1) \quad (1,2) \quad (1,3)$$

$$(2,0) \quad (2,1) \quad (2,2) \quad (2,3)$$

Send each element (x, y) to $4x + y$ and you have \mathbb{Z}_{12}

2.3.3 Automorphisms

Definition 2.21. An automorphism of a group G is an isomorphism from G to G . The set of all automorphisms forms a group under composition of functions, which is called the automorphism group of G and written $\text{Aut}(G)$.

Automorphisms fix the identity and send generators to generators.

Example 2.22. Consider the automorphisms of \mathbb{Z}_4 . There are only two generators in this group: 1 and 3. Therefore, there are only two elements in $\text{Aut}(\mathbb{Z}_4)$: the trivial one, and the one that flips 1 and 3.

2.4 Products

2.4.1 Direct Products

Theorem 2.23. The set $G \times H$ of two groups G and H is a group that consists of the elements (g, h) where $g \in G$ and $h \in H$. Given two elements (g, h) and (g', h') of $G \times H$, multiplication on this group is defined by

$$(g, h)(g', h') = (gg', hh')$$

where the first term, gg' , inherits the multiplication of G , and the second, hh' , inherits the multiplication of H . We call this group the direct product $G \times H$ of G and H .

Proof. Associativity follows from the associativity in both G and H . The identity is (e, e) and the (g^{-1}, h^{-1}) is the inverse of (g, h) .

Example 2.24. Consider $\mathbb{Z}_4 \times \mathbb{Z}_2$. This group has 8 elements: $(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)$.

Multiplication is defined by

$$(x, y) + (x', y') = (x + 4x', y + 2y')$$

2.4.2. Semidirect Products

Theorem 2.25. Suppose we have the groups G, H and the homomorphism $\phi : G \rightarrow \text{Aut}(H)$. Then the “twisted” direct product forms a new group. Its elements are of the form (g, h) with $g \in G$ and $h \in H$ and multiplication is defined by

$$(g, h)(g', h') = (g \cdot \phi(h)(g'), h \cdot h').$$

We call this group the semidirect product of G and H .

Example 2.26. Consider the semidirect product $\mathbb{Z}_4 * \mathbb{Z}_2$. The elements in this group are the same as those in $\mathbb{Z}_4 \times \mathbb{Z}_2$ as listed in Example 2.24.

We need to define ϕ . There are only two automorphisms of \mathbb{Z}_4 as shown in Example 2.22. Let the trivial automorphism be denoted with e and the other with σ . Then, since $\phi: \mathbb{Z}_2 \rightarrow \text{Aut}(H)$, we have $\phi(0) = e$ and $\phi(1) = \sigma$.

Now we can perform multiplication on the group. Consider multiplying the elements $(0, 0)$ and $(1, 0)$. Since $\phi(0) = e$ this multiplication is just like that of the direct product:

$$(0, 0)(1, 0) = (0 + \phi(0)1, 0 + 0) = (0 + e(1), 0 + 0)(1, 0)$$

Now consider the elements $(1, 0)$ and $(0, 1)$.

$$(0, 1)(1, 0) = (0 + \phi(1)(1), 1 + 0) = (0 + \sigma(1), 1 + 0) = (3, 1)$$

2.4.3. Wreath Products

The generalized form of a wreath product $G \wr H$ is too complicated for the scope of this paper. Therefore, we will only consider the special case taking a wreath product with \mathbb{Z}_2 .

Consider the group G . Then $G \wr \mathbb{Z}_2$ is isomorphic to $(G \times G) * \mathbb{Z}_2$. We will discuss this semidirect product in the dihedral notation as in Example 2.27. Thus, let the elements of $G \times G$ be denoted by $r_1^m r_2^n$.

The automorphism for a wreath product must permute the parts of an element in $G \times G$. Since we only have two elements, r_1^m and r_2^n , the only non-trivial automorphism is to switch them. That is $\delta(r_1^m r_2^n) = r_2^n r_1^m$. Thus,

$$r_1^m r_2^n s = s \delta(r_1^m r_2^n) = s r_2^n r_1^m$$

3. Music Theory

Music theory is a tool and framework with which we explain our listening experience. However, both the tool and the term “listening experience” are loosely defined. They are dependent on the music.

During the mid-15th century, composers began constructing their pieces around a particular pitch, called the tonic. This pitch was quickly established at the start of the piece and all other pitches were heard relative to it. Intervals and chords were labeled as consonant or dissonant. A feeling of tension occurred in various ways, such as when resolution was delayed, or when the music leapt to

distant keys (more than two accidentals removed from the tonic). Resolution to the tonic was crucial to ending the piece. After over two centuries of tonal music, listeners have begun to expect music to resolve in particular ways.

Along with the development of tonal music was the development of tonal theory. Its structure and notation allowed theorists to describe the listener's expectation. Thus, it provided an explanation for our reaction to particular harmonies. It explained our feeling of surprise at a particular chord and our feeling of finality at the end of a piece.

Around the turn of the 19th century, composers pushed the boundaries of tonal music. They began using dissonant chords with unprecedented freedom and resolved them in new ways. Eventually, their pieces no longer fit the framework of tonal music. Tonal theory no longer provided an adequate explanation for our listening experience. Thus, a new framework was constructed called atonal music theory.

Discussions in music require a certain vocabulary. The following terms are defined in the appendix:

- interval
- half step (semitone) & whole step (whole tone), flat, sharp, natural & accidental
- enharmonic equivalence
- major, minor, mode
- parallel & relative
- scale degree
- triad

3.1. Basic concepts of atonal music theory

Atonal music is based on sequences of pitches and intervals. No particular pitch is considered more important than the others and resolution of dissonance is unimportant. It assumes octave and enharmonic equivalence.

Definition 3.1. Pitches that are separated by an integer multiple of an octave, or are enharmonically equivalent belong to the same pitch class.

Definition 3.2. Consider the pitches a and b . The ordered pitch-class interval from a to b is $a-b \pmod{12}$.

Definition 3.3. A pitch-class set is an unordered set of pitch-classes, denoted as a string of integers enclosed in brackets. Within a pitch-class set, we do not have information about the register, rhythm or order of the pitches.

Example 3.4. The C major triad consists of the notes C, E and G. This can be represented as the pitch-class set [047], since $C = 0$, $E = 4$ and $G = 7$.

In atonal music, operations are performed on pitch-class sets, creating new pitch-class sets that are spread throughout the music. Thus, the music sounds random and yet structured at the same time. We will discuss two types of operations in this paper: the transpositions and the inversions.

3.1.1 T_n , the Transpositions

Definition 3.5. The transposition T_n moves a pitch-class or pitch-class set up by $n \pmod{12}$. (Note: moving down by n is equivalent to moving up by $12-n$.)

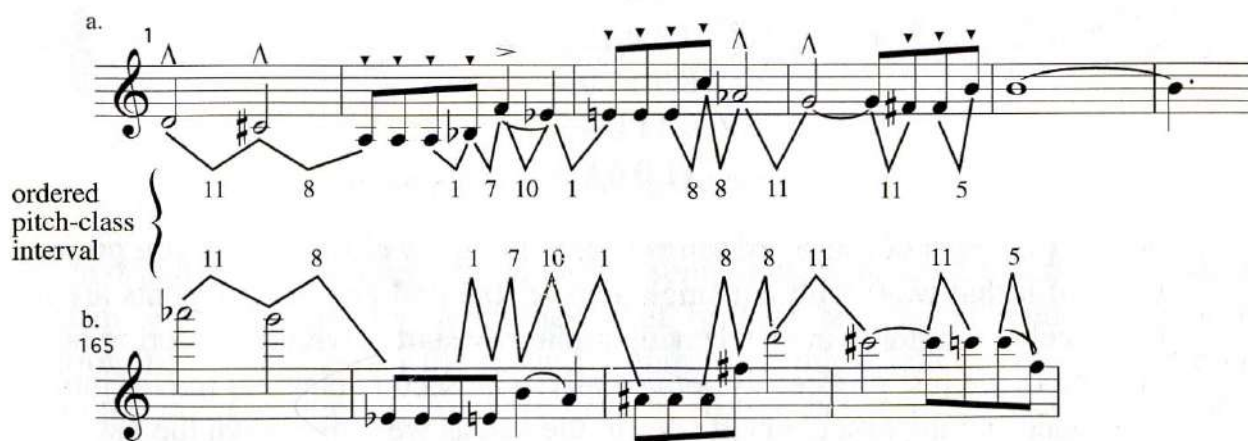


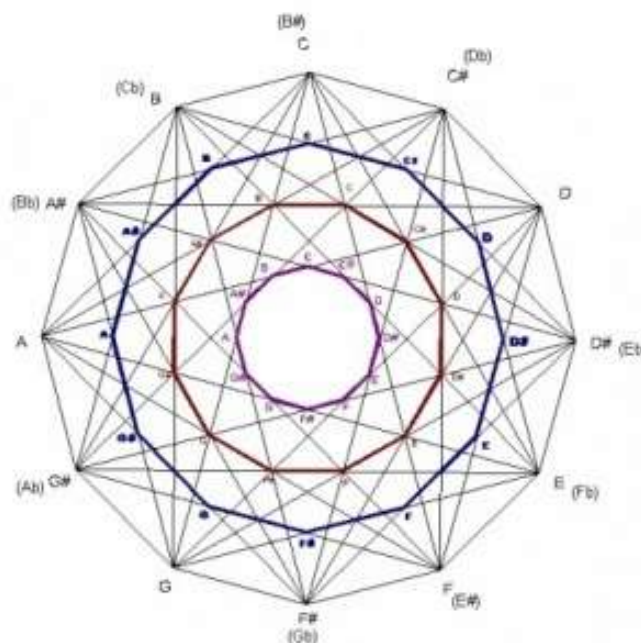
Figure 1: Two lines of pitch classes related by T6 (Schoenberg, String Quartet No. 4).

3.1.2 TnI, the Inversions

Definition 3.6. Consider the pitch a . Inversion $T_n I$ inverts the pitch about $C(0)$ and then transposes it by n . That is, $T_n I(a) = -a + n(\text{mod } 12)$.

4. Group Theory as a Structure for Atonal Music Theory

The numbering of the pitch classes reveals their isomorphism to \mathbb{Z}_{12} . More interestingly, the group of transpositions and inversions, denoted $T_n/T_n I$ is isomorphic to the dihedral group D_{12} .



Sehr langsam $\text{♩} = \text{ca. } 40$

Fl. 1 5

Ob.

Cl. 3

Trp. 1 Immer mit Dmpf. pp

Vln. 2 mit Dmpf. p

Vla. pp

Piano pp p pp 4

1 2 3 4

Figure 3: Transpositionally equivalent pitch-class sets (Webern, Concerto for Nine Instruments, Op. 24).

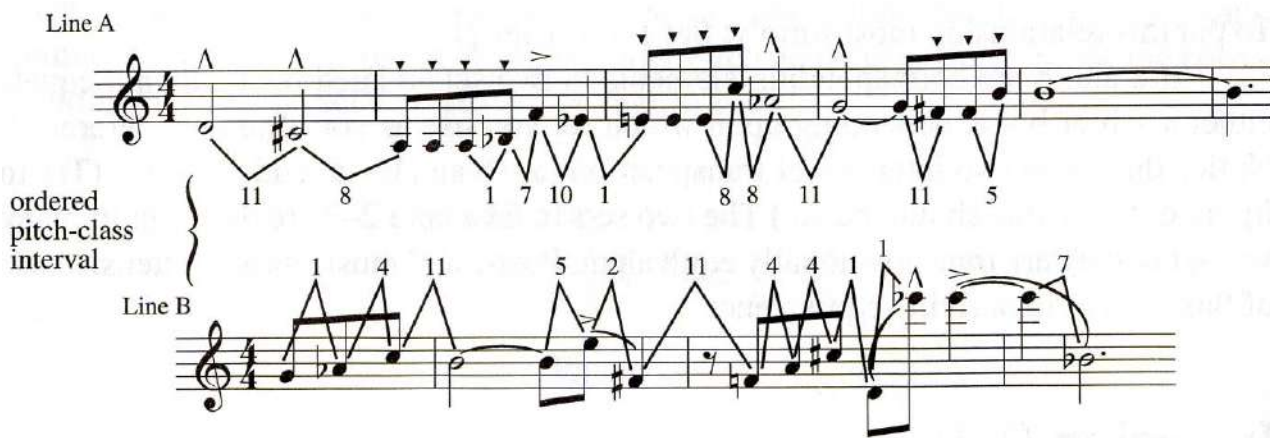


Figure 4: Two lines of pitch classes related by T9I (Schoenberg, String Quartet No. 4)

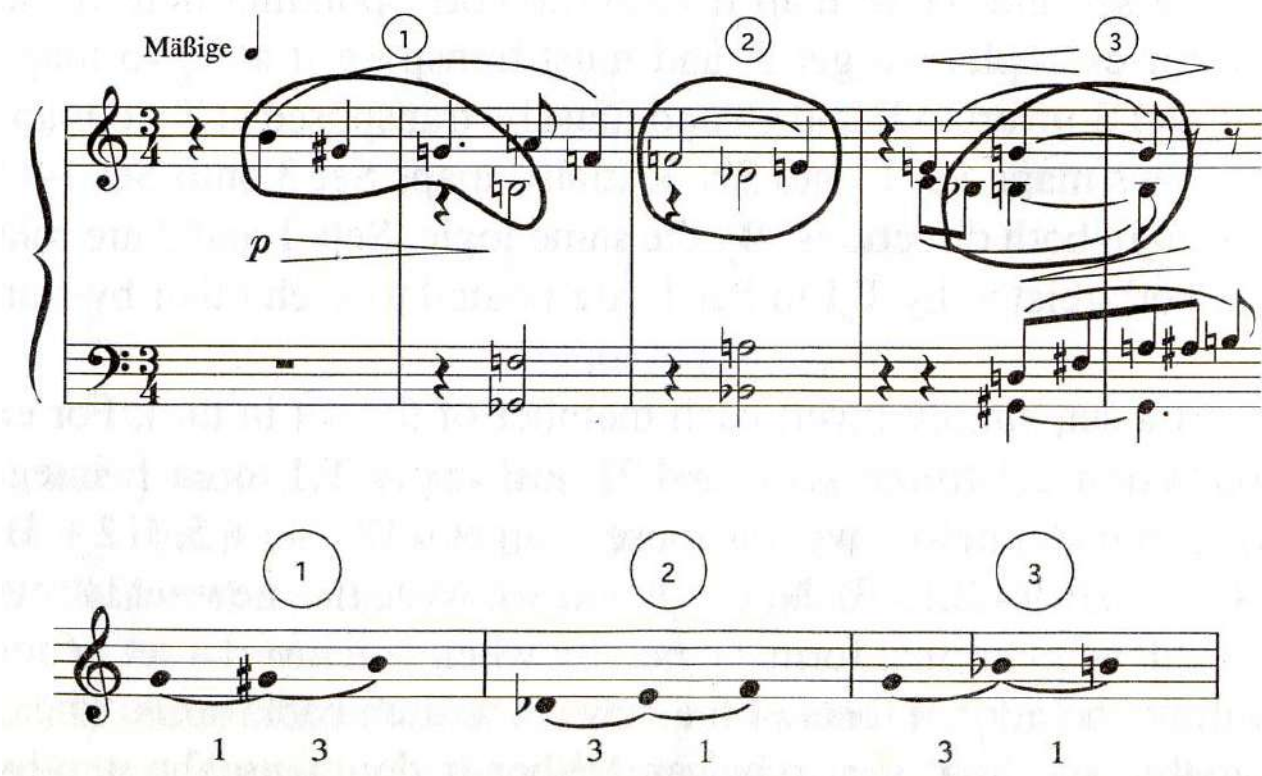


Figure 5: Inversionally equivalent pitch-class sets (Schoenberg, Piano Piece, Op. 11, No. 1)

5. A Flaw in Atonal Music Theory

Consider the operation that changes a major triad to a minor triad. To our ears, this is the same operation regardless of whether we start with a CM triad or a DM triad. However, consider the CM triad as the pitch class [047], cm as [037], DM as [269] and dm as [259]. Then, we have

$$\text{CM} \rightarrow \text{cm} = [047] \rightarrow [037] = \text{T7I} \quad \text{DM} \rightarrow \text{dm} = [269] \rightarrow [259] = \text{T11I}$$

This is a misleading representation of the music, because our ears do not hear two different actions. Therefore, the structure of atonal music theory has an inherent flaw. It cannot support these simple transformations.

A music theorist named Hugo Riemann recognized this problem. He invented the idea of a “triadic transformation.” Later music theorists devised three operations, called Neo-Riemannian operations, that functioned specifically on triads:

- The Parallel operation (P) moves the middle note of a triad up or down a semitone such that a major triad becomes minor and a minor triad becomes major. For example, it would move the E in a CM to an E \flat and the E \flat in a cm triad to an E \natural .
- The Leading-tone exchange (L) moves the bottom note of a major triad down a semitone and the top note of a minor triad up a semitone. Thus, a CM triad would turn into an em triad, and a cm triad would turn into an A \flat M triad.
- The Relative operation (R) sends a chord to its relative counterpart by moving the top note of a major triad up by a whole tone, and moving the bottom note of a minor triad down by a whole tone. Thus, a CM triad would turn into an am triad, and a cm triad would turn into an E \flat M triad.

These three were particularly interesting because they allowed for parsimonious voice-leading. That is, in moving from one triad to another, only one voice (top, middle or bottom) moved, and it moved by nothing more than a whole step. In addition, they allowed a transformation from any one chord to another by composition of these operations.

6. Uniform Triadic Transformations

This P, L and R notation, while a definite improvement, could still be unclear, unwieldy and limited in its usefulness. For example, a move from a CM triad to a b \flat m triad requires a minimum of six Neo-Riemannian operations. Furthermore, there are nine different ways to write it in six operations: LPRPR, LRPRP, PLRLR, PRLRP, PRPRL, RLPLR, RLRLP, RPLPR, RPRPL. Of course, there are even more ways to write it in more than six operations. Not only has this notation become pedantic, it also fails to reflect the music: who would hear six operations in a simple move from CM to b \flat m?

To resolve this problem, another music theorist named Julian Hook devised a new notation for transformations on triads, which he called uniform triadic transformations (UTTs). This notation, in fact, was a group structure with intriguing algebraic properties. Before we jump into a discussion on

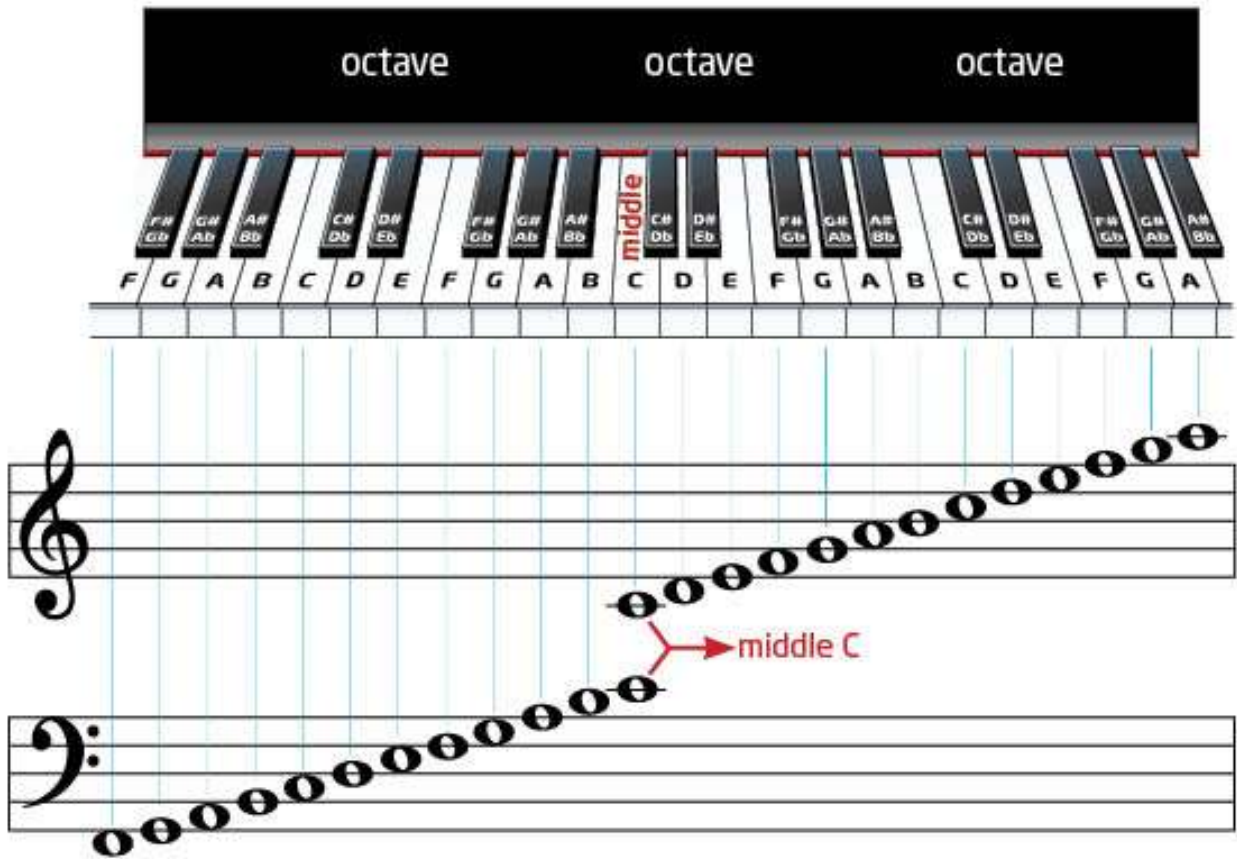


Figure 6: A piano with the keys placed onto the music staff

Definition 6.1. A triad is an ordered pair $\Delta = (r, \sigma)$ where r is the root of the triad expressed as an integer (mod 12), and σ is a sign representing its mode (+ for major, - for minor).

Example 6.2. $\Delta = (0, +)$ represents a C major triad and $\Delta = (6, -)$ represents an f# minor triad.

Theorem 6.3. The set of all 24 major and minor triads, forms a abelian group with multiplication defined by

$$(t_1, \delta_1)(t_2, \delta_2) = (t_1 + t_2, \delta_1\delta_2)$$

We call this set Γ .

Proof. This group is clearly isomorphic to $\mathbb{Z}_{12} \times \mathbb{Z}_2$, which by Theorem 2.23 is a group.

Definition 6.4. Given $\Delta_1 = (r_1, \delta_1)$ and $\Delta_2 = (r_2, \delta_2)$, the transposition level $t = r_2 - r_1$ is the interval between the roots and the sign factor $\delta = \delta_1\delta_2$ is the change in sign. (δ is multiplied as expected with $++ = +, +- = -, -+ = -$ and $-- = +$.) The Γ -interval $\text{int}(\Delta_1, \Delta_2)$ is the ordered pair (t, δ) where t and δ are the transposition level and sign factor as defined above.

Example 6.5. The Γ -interval from $(0, +)$ (C major) to $(6, -)$ (f# minor) is $(6, -)$.

6.1. Introduction to Triadic Transformations

Definition 6.6. A triadic transformation is a bijective mapping from Γ to itself. In other words, it is a permutation of Γ .

Theorem 6.7. The set of all triadic transformations forms a group G . Proof. After numbering the triads, this group is clearly isomorphic to S_{24} .

The order of G is huge: 24 factorial. However, most of these transformations have little musical meaning since the action of a transformation on one triad may not resemble its action on another triad.

6.2. V, the Uniform Triadic Transformations

Of particular musical interest are the UTTs because they operate on all major triads in the same manner. Similarly, the UTTs have one action for all minor triads.

Definition 6.8. Consider the triadic transformation that transforms (r, σ) to (r', σ') . It is a uniform triadic transformation (UTT) if it transforms $(r + t, \sigma)$ to $(r' + t, \sigma')$ $\forall t \in \mathbb{Z}_{12}$.

It is important to note that not all musically interesting transformations are UTTs. The inversions TnI , for example, are not part of the UTTs.

Any UTT is completely determined by three parameters:

- t^+ , its transposition level for a major triad
- t^- , its transposition level for a minor triad
- σ , its sign. (Note: it may seem that σ could be different for major and minor triads. However, in order to be a transformation, a UTT must map Γ to itself. Thus, if it switches major triads to minor, it must switch minor triads to major. That is $\delta^+ = -\delta^-$. Positive σ implies no change in mode (it is **mode-preserving**), negative σ implies switching to the opposite mode (it is **mode-reversing**).)

We can thus denote any UTT U by the ordered triple $U = \langle \sigma, t^+, t^- \rangle$. Example 6.9. We will convert Riemann's P, L and R in UTT notation:

$$P = \langle -, 0, 0 \rangle \quad L = \langle -, 4, 8 \rangle \quad R = \langle -, 9, 3 \rangle$$

Note, Hook uses left-to-right orthography. Thus, $U_1 U_2$ implies “first U_1 then U_2 .” As usual, $U^2 = U U$, etc. Although it is less intuitive for mathematicians, we will adhere to his notation.

6.2.1 Multiplication on V

Multiplication on V should clearly be composition. Before we derive a general formula for the composition of two UTTs, let us consider some concrete examples.

Example 6.10. Consider the UTTs $U = \langle +, 4, 7 \rangle$ and $V = \langle -, 5, 10 \rangle$. Let us calculate the product $UV = \langle \delta_{UV}, t_{UV}^+, t_{UV}^- \rangle$. When UV acts on a CM triad ($\Delta = (0, +)$) we have:

$$(0, +) \xrightarrow{U} (4, +) \xrightarrow{V} (9, -)$$

Thus, UV transforms the major triads through the Γ -interval (9, -). We can deduce that $\delta_{UV} = -$ and $t_{UV}^+ = 9$.

When UV acts on a cm triad ($\Delta = (0, -)$) we have:

$$(0, -) \xrightarrow{U} (7, -) \xrightarrow{V} (5, +)$$

Thus, UV transforms the minor triads through the Γ -interval (5, +) and $t_{UV}^- = 5$. Hence, $UV = \langle -, 9, 5 \rangle$

This product may be calculated by multiplying the signs ($\delta_{UV} = \delta_U \delta_V$) and adding the corresponding transposition levels ($t_{UV}^+ = t_U^+ + t_V^+$; $t_{UV}^- = t_U^- + t_V^-$). Figure 6 depicts a visual representation of UV.

Example 6.11. Now consider the product VU. In this case we have

$$(0, +) \xrightarrow{V} (5, -) \xrightarrow{U} (0, -)$$

and

$$(0, -) \xrightarrow{V} (10, +) \xrightarrow{U} (2, +)$$

Therefore, $VU = \langle -, 0, 2 \rangle$. In this case, the signs were multiplied as before, the transposition levels were “cross-added.” That is, $t_{UV}^+ = t_U^+ + t_V^-$ and $t_{UV}^- = t_V^+ + t_U^-$.

We can see that in the above example, the “cross-adding” was due to the sign of the first transformation. In the first case, the first UTT (U) was mode-preserving, so the second UTT (V) acted on the same mode as U. Thus, the corresponding transposition levels were applied in succession. In the second case, the first UTT (V) was mode-reversing, so the second UTT (U) acted on the opposite mode as V and opposite transposition levels were combined. This leads us to the general form of UTT multiplication:

Theorem 6.12. Consider two UTTs $U = \langle \delta_U, t_U^+, t_U^- \rangle$ and $V = \langle \delta_V, t_V^+, t_V^- \rangle$. Multiplication on V is given by $UV = \langle \delta_U \delta_V, t_U^+ + t_V^{(\delta_U)}, t_U^- + t_V^{(-\delta_U)} \rangle$

The reader can verify that following the process above using two arbitrary elements in V will give the desired result.

6.2.2 Inversion on V

Again, before we derive a general formula for the inverse of a UTT, let us consider some concrete examples.

Example 6.13. Consider the UTT $U = \langle +, 4, 7 \rangle$. Because $(0, +) \xrightarrow{U} (4, +)$ and $(0, -) \xrightarrow{U} (7, -)$, we need $(4, +) \xrightarrow{U^{-1}} (0, +)$ and $(7, -) \xrightarrow{U^{-1}} (0, -)$. Thus, $U^{-1} = \langle +, 8, 5 \rangle$. Note how this is simply the inversion of the transposition levels: $\langle +, -4 \pmod{12}, -7 \pmod{12} \rangle$.

Example 6.14. Now consider the UTT $V = \langle -, 5, 10 \rangle$. $(0, +) \xrightarrow{V} (5, -)$ and $(0, -) \xrightarrow{V} (10, +)$. Thus, $(5, -) \xrightarrow{V^{-1}} (0, +)$ and $(10, +) \xrightarrow{V^{-1}} (0, -)$. Therefore, $V^{-1} = \langle -2, 7 \rangle$ or $\langle -, -10 \pmod{12}, -5 \pmod{12} \rangle$. In this case, the transposition levels are not only inverted, but interchanged. Once again, this is due to the sign of V .

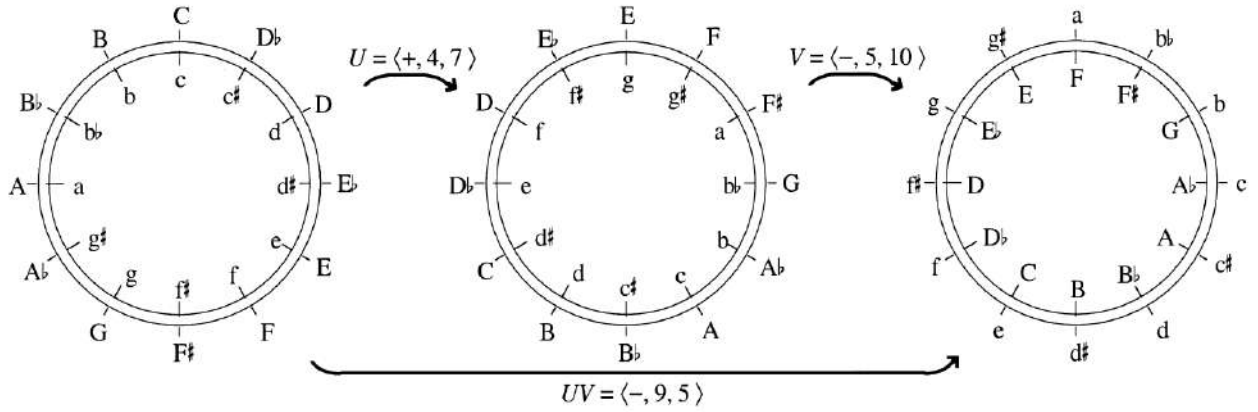


Figure 7: Visual representation of the UTT equation $\langle +, 4, 7 \rangle \langle -, 5, 10 \rangle = \langle -, 9, 5 \rangle$

Theorem 6.16. The set V of UTTs is a group that is isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$

Proof. Remember from Section 2.4.3 how we represented $G \times G$ in the form $r_1^m r_2^n$. Let G be \mathbb{Z}_{12} and let us switch the 1 and 2 to + and -. Then the elements of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ are $s r_+^m r_-^n$ where $m, n \in \mathbb{Z}_{12}$.

Also note that the transpositions, which are equivalent to the transposition levels of a UTT, are isomorphic to the rotations of the D_{12} by $T_n \rightarrow r^n$. We initially wrote that the $T_n/T_n I$ group was isomorphic by $T_n \rightarrow r^{12-n}$. This reflected our visual representation of the two groups. However, the groups are still isomorphic if we choose $T_n \rightarrow r^n$, which makes the following argument clearer.

It seems likely that the UTTs are isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ by $\langle \sigma, t^+, t^- \rangle \rightarrow s r_+^m r_-^n$. We have already shown that the UTTs have multiplication and inverses. We only need to show that it follows the multiplication of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$. That is, $(r_+^m r_-^n)s = s(r_-^n r_+^m)$.

$$\begin{aligned}
 (r_+^m r_-^n)s &= (e r_+^m r_-^n)(see) \\
 &= \langle -, 0, 0 \rangle \langle +, t_m^+, t_n^- \rangle \\
 &= \langle -, 0 + t_n^-, 0 + t_m^+ \rangle \\
 &= \langle -, t_n^-, t_m^+ \rangle \\
 &= s(r_-^n, r_+^m)
 \end{aligned}$$

Thus, multiplication is preserved and the isomorphism holds.

6.2.3 Even and Odd UTTs

UTTs can be classified as “even” or “odd” in multiple ways. Let us begin with “even/odd in the sense of total transposition.”

Definition 6.17. We say that a UTT $U = \langle \sigma, t^+, t^- \rangle$ is even (or, more fully, even in the sense of total transposition) if its total transposition $\tau(U) = t^+ + t^-$ is an even number. U is odd (in the sense of total transposition) if $\tau(U)$ is an odd number.

Definition 6.19. A UTTs is even (in the sense of permutation theory) if it can be written as a product of an even number of 2-cycles and odd (in the sense of permutation theory) if it can be written as a product of an odd number of 2-cycles.

It is remarkable that the two definitions of even or odd (in the sense of total transposition versus permutation theory) are actually equivalent.

Theorem 6.20. A UTT is even in the sense of total transposition if and only if it is even in the sense of permutation theory.

6.3. \mathbb{R} , the Riemannian UTTs

Recall the Neo-Riemannian operators P , L and R as introduced in Section 5 and written as UTTs in Example 6.9. For each, the transposition level for a major triad is equal and opposite that of a minor triad. We define the Riemannian UTTs as follows.

Definition 6.21. A Riemannian UTT is a UTT such that $t^+ = -t^-$.

Theorem 6.22. The set of \mathbb{R} of Riemannian UTTs is isomorphic to D_{12} .

Proof. D_{12} can be defined as the group of order 24 generated by s and r , such that $s^2 = e$, $r^{12} = e$ and $sr = r^{-1}s$

The generators of \mathbb{R} are $\langle -, 0, 0 \rangle$ and $\langle +, 1, 11 \rangle$.

$$(\langle -, 0, 0 \rangle)^2 = \langle -, 0+0, 0+0 \rangle = \langle +, 0, 0 \rangle = e \in \mathbb{R}$$

$$(\langle +, 1, 11 \rangle)^{12} = \langle +, 12 \cdot (1), 12 \cdot (11) \rangle = \langle +, 0, 0 \rangle = e$$

$$(\langle +, 1, 11 \rangle)^{-1} = \langle +, 11, 1 \rangle$$

$$\langle -, 0, 0 \rangle \langle +, 1, 11 \rangle = \langle -, 0 + 11, 0 + 1 \rangle = \langle -, 11 + 0, 1 + 0 \rangle$$

$$= \langle +, 1, 11 \rangle \langle -, 0, 0 \rangle = r^{-1}s$$

6.4 \mathbb{K} , the Subgroups of \mathbb{V}

Generally, it is difficult to list all the subgroups of a given group G . However, it is possible to list all the subgroups of \mathbb{V} .

Definition 6.23. Give two integers a and b (mod 12), we define three subsets of \mathbb{V} as follows.

- $K^+(a)$ is the set of all mode-preserving UTTs of the form $\langle +, n, an \rangle$ as n ranges through the integers mod 12.

- $K^-(a, b)$ is the set of all mode-reversing UTTs of the form $\langle -, n, an+b \rangle$.
- $K(a, b) = K^+(a) \cup K^-(a, b)$

Theorem 6.24. $K(a, b)$ is a subgroup of V if and only if the numbers a and b satisfy $a^2=1$ and $ab = b \pmod{12}$.

The condition $a^2 = 1$ is satisfied only for $a = 1, 5, 7$ and 11 . If $a = 1$ then the condition $ab = b$ is automatically satisfied. For other values of a , the allowable values of b are different in each case. The following is a complete list of the groups $K(a, b)$:

$K(1,0), K(1,1), K(1,2), \dots, K(1,11)$
 $K(5, 0), K(5, 3), K(5, 6), K(5, 9)$
 $K(7, 0), K(7, 2), K(7, 4), K(7, 6), K(7, 8), K(7, 10) K(11, 0), K(11, 6)$

7. Musical Application

The UTTs of order 24 are of considerable musical interest. When such a transformation is applied repeatedly, the resulting chain of triads will cycle through all 24 major and minor triads before returning to the original one. Take, for example, the UTT $U = \langle -, 9, 8 \rangle$. Its repeated application produces a chain in the scherzo of Beethoven's Ninth Symphony :

$$C \xrightarrow{U} a \xrightarrow{U} F \xrightarrow{U} d \rightarrow \dots \xrightarrow{U} A$$

This chain is 19 triads long, only five short of a complete cycle.

Such triad chains are rarely prolonged to this extent. There are, however, examples from literature that circumnavigate the entire cycle of 24 triads. These are found in collections of pieces such as Bach's Well-Tempered Clavier and the Chopin Preludes.

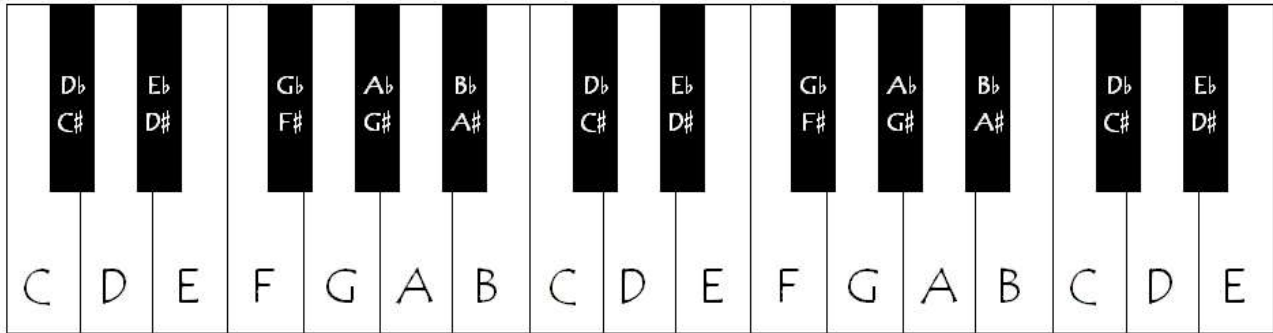


Figure 8: A piano with the keys labeled

8. Conclusion

We can see that Hook's UTTs not only have interesting mathematical properties, but also musical significance. Musically, the choice of triads is non-arbitrary since triads occur throughout music. Mathematically, however, the set choice is arbitrary. Some current research in music theory investigates the generalization Hook's UTTs to larger chords or even to pitch-class sets. The flexibility these generalisations will provide may greatly improve atonal analysis.

References

- [1] Armstrong, M. Groups and Symmetry. Springer-Verlag, 1988.
- [2] Dummit, D. S., and Foote, R. M. Abstract Algebra, third ed. Wiley, 2003.
- [3] Hook, J. Uniform triadic transformations. *Journal of Music Theory* 46, 1-2 (2002), 57–126.
- [4] Straus, J. N. Introduction to Post-Tonal Theory, second ed. Prentice-Hall, Inc., 2000.

***RAMAKRISHNA MISSION VIVEKANANDA CENTENARY
COLLEGE***

- **Name: Amit Kumar Ghosh**
- **Reg no: A01-1152-113-029-2019**
- **Roll: 2022151113**
- **College roll: 343**
- **Topic: Cayley's theorem by group homomorphism and
Group action**
- **Supervised by: Prof. Pravanjan Kumar Rana**

ACKNOWLEDGEMENT

We would like to express my special thanks of gratitude to our group theory teacher “Mr. Pravanjan Kumar Rana” for his able guidance and support in completing this project.

I would also like to extend my gratitude to principal “swami Kamalasthanada maharaj” for providing me with all facility that was required.

Date:

15-01-2022

Amit Kumar Ghosh (2022151113)

Sanjay Karmakar (2022151111)

Souvik Pal (2022151118)

- **CONTENTS:**

- **Definition of group action**
- **Definition of group homomorphism**
- **Induced homomorphism**
- **Cayley's theorem**
- **Proof by Cayley's theorem
(by group homomorphism method)
(by group action method)**

TOPIC: CAYLEY'S THEOREM BY GROUP HOMOMORPHISM AND GROUP ACTION

Definition of Group Action:

Let G be a group and X be a set. Then G is said to act on X if there is a mapping $\phi: G \times X \rightarrow X$, with $\phi(a, x)$ written $a * x$ such that for all $a, b \in G, x \in X$

- $a * (b * x) = ab * x$
- $e * x = x$

The mapping ϕ is called **the action of G on X** , and X is said to be a G -set.

Definition of Group homomorphism:

Let $(G, *)$ and (G', \circ) be two groups and f be a function from G into G' . Then f is called a **group homomorphism** of G to G' if for all $a, b \in G$,

$$f(a * b) = f(a) \circ f(b)$$

Theorem:

Let G be a group and let X be a set.

- If X is a G -set, then the action of G on X induces a homomorphism $\phi: G \rightarrow S_X$.
- Any homomorphism $\phi: G \rightarrow S_X$ induces an action of G onto X .

Proof:

At first we define $\phi: G \rightarrow S_X$ by $(\phi(a))(x) = ax$, $a \in G, x \in X$

Now we have to prove $\phi(a) \in S_X$

Let $x_1, x_2 \in X$

Then,

$$(\phi(a))(x_1) = (\phi(a))(x_2)$$

$$\Rightarrow ax_1 = ax_2$$

$$\Rightarrow x_1 = x_2$$

$\therefore \phi(a)$ is one-one.

Now,

$$\begin{aligned} x_2 &= a(a^{-1}x_2) \\ &= (\phi(a))(a^{-1}x_2) \quad , a^{-1}x_2 \in X \end{aligned}$$

Thus, $\phi(a) \in S_X$

Now, let, $a, b \in G$

Then

$$\begin{aligned} \phi(ab)(x) &= (ab)(x) \\ &= a(bx) \\ &= a(\phi(b)(x)) \\ &= \phi(a)\phi(b)(x) \quad , \forall x \in X \end{aligned}$$

Here, $\phi(ab) = \phi(a)\phi(b)$

So, ϕ is a homomorphism.

Now we define,

$$a * x = \phi(a)(x)$$

That is $ax = (\phi(a))(x)$

Let, $a, b \in G$

Then

$$\begin{aligned}(ab)(x) &= (\phi(ab))(x) \\ &= (\phi(a)\phi(b))(x) \\ &= \phi(a)(\phi(b)(x)) \\ &= \phi(a)(bx) \\ &= a(bx)\end{aligned}$$

Also $ex = (\phi(e))(x) = e$ (where e is the identity element)

Hence X is a G -set.

Application: Cayley's Theorem:

Let G be a group. Then G is isomorphic to a subgroup of group S_G .

Proof by group action method:

Here we want to prove this theorem by the group action method.

G is a G -set.

Where G acts on G by group operation.

This left action induces a homomorphism $\phi: G \rightarrow S_G$

Where $(\phi(a))(x) = ax \quad a \in G, x \in G$

$$\begin{aligned}\text{Ker } \phi &= \{a \in G : \phi(a) = \text{identity permutation on } G\} \\ &= \{a \in G : ax = x, \forall x \in G\} \\ &= \{e\}\end{aligned}$$

Hence ϕ is a monomorphism.

Now by first isomorphism theorem $\frac{G}{\text{ker } \phi} \cong \text{subgroup of } S_G$

So, the theorem is proved.

Proof by group homomorphism method:

Here we want to prove this theorem by the homomorphism method.

Let G be a group.

For any $a \in G$ the mapping $f_a : G \rightarrow G$, given by $f_a(x) = ax$ for all $x \in G$ is a bijection, because,

$$\begin{aligned} ax &= ax' \\ \Rightarrow x &= x' \end{aligned}$$

And $y = f_a(a^{-1}y)$ for all $x, x', y \in G$

Considering the mapping, $\phi : G \rightarrow S_G$

Where $\phi(a) = f_a$ for all $a \in G$

Where S_G is a symmetric group on the set G

Now, for all $a, b, x \in G$,

$$\begin{aligned} f_{ab}(x) &= abx \\ &= f_a(bx) \\ &= f_a(f_b(x)) \\ &= (f_a f_b)(x) \end{aligned}$$

Hence $\phi(ab) = \phi(a)\phi(b)$

Therefore, ϕ is a homomorphism.

And $\text{Im } \phi$ is a subgroup of S_G

Moreover,

$$\begin{aligned} \phi(a) &= \phi(b) \\ \Rightarrow ax &= bx \quad \forall x \in G \\ \Rightarrow a &= b \end{aligned}$$

Hence ϕ is an injective homomorphism.

Therefore G is isomorphic to a subgroup of S_G

The above isomorphism is called the *left regular representation* of G .

Similarly, we have a right regular representation.

Reference:

To write this project, we take help of these following books,

- Abstract Algebra (Dummit, David, Foote)
- Contemporary abstract algebra (Joseph Gallian)
- Fundamentals of Abstract Algebra (Malik, Moderesen, Sen)

Project on External Direct Product

Prepared by

- 1) AKRAM KHAN (356)
- 2) SUMIT PARAMANIK (333)
- 3) AGNIVA BANERJEE (332)

External Direct Product and its application

Abstract:-

External direct product is one of the most important part of group theory .We are going to introduce an idea how the external direct product help us in data science , public Key Cryptography,digital signature ,genetics and electrical circuits .

Introduction:-

In this project, we show how to piece together groups to make large groups. Previously, we will show that we can often start with one large group and decompose it into a product of smaller groups in much the same way as a composite positive integer can be broken down into a product of primes. These methods will later be used to give us a simple way to construct all finite abelian groups.

Definition :

Let G_1, G_2, \dots, G_n be a finite collection of groups. The external direct product of G_1, G_2, \dots, G_n , written as $G_1 \times G_2 \times \dots \times G_n$, is the set of all n -tuples for which the i th component is an element of G_i and **the operation is component wise.**

The resulting algebraic object satisfies the axioms for a group. Specifically:

Associativity :-

The binary operation on $G \times H$ is associativity.

Identity :-

The direct product has an identity element, namely $(1_G, 1_H)$, where 1_G is the identity element of G and 1_H is the identity element of H .

Inverses :-

The inverses of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}) , where g^{-1} is the inverse of g in G , and h^{-1} is the inverse of h in H .

Hence, external direct product form a group.

In symbols, $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}$, Where $(g_1, g_2, \dots, g_n)(g_1', g_2', \dots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \dots, g_n g_n')$. It is understood that each product $g_i g_i'$ is performed with the operation of G_i . We leave it to the reader to show that the external direct product of groups is itself a group.

Properties of external direct product:-

1. Order of $(G_1 \times G_2 \times G_3 \times \dots \times G_k) = |G_1| \cdot |G_2| \cdot |G_3| \cdot \dots \cdot |G_k|$

2. The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols, $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$.

Proof : Denote the identity of G_i by e_i . Let $s = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$ and $t = |(g_1, g_2, \dots, g_n)|$. Because s is a multiple of each $|g_i|$ implies that $(g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (e_1, e_2, \dots, e_n)$, we know that $t \leq s$. On the other hand, from $(g_1, g_2, \dots, g_n)^t = (g_1^t, g_2^t, \dots, g_n^t) = (e_1, e_2, \dots, e_n)$ we see that t is a common multiple of $|g_1|, |g_2|, \dots, |g_n|$. Thus, $s \leq t$. If $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$ is an external direct product, say $(g_1, g_2, g_3, \dots, g_k) \in \text{EDP}$ Now, $(g_1, g_2, g_3, \dots, g_k)$ is just an element of $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$

Application :-

We conclude this project with five applications of the material presented here—three to cryptography, the science of sending and deciphering secret messages, one to genetics, and one to electric circuits.

Data Security :-

Because computers are built from two-state electronic components, it is natural to represent information as strings of 0s and 1s called binary strings. A binary string of length n can naturally be thought of as an element of $Z_2 \times Z_2 \times \dots \times Z_2$ (n copies) where the parentheses and the commas have been deleted. Thus the binary string 11000110 corresponds to the element $(1, 1, 0, 0, 0, 1, 1, 0)$ in $Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$. Similarly, two binary strings $a_1 a_2 \dots a_n$ and $b_1 b_2 \dots b_n$ are added component wise modulo 2 just as their corresponding elements in $Z_2 \times Z_2 \times \dots \times Z_2$ are. For example,

$$11000111 + 01110110 = 10110001$$

And,

$$10011100 + 10011100 = 00000000.$$

The fact that the sum of two binary sequences $a_1a_2 \dots a_n = b_1b_2 \dots b_n = 00 \dots 0$ if and only if the sequences are identical is the basis for a data security system used to protect internet transactions.

Suppose that you want to purchase a compact disc from **www.Amazon.com**. Need you be concerned that a hacker will intercept your credit-card number during the transaction? As you might expect, your credit-card number is sent to Amazon in a way that protects the data. We explain one way to send credit-card numbers over the Web securely. When you place an order with Amazon the company sends your computer a randomly generated string of 0's and 1's called a key. This key has the same length as the binary string corresponding to your credit-card number and the two strings are added (think of this process as "locking" the data). The resulting sum is then transmitted to Amazon. Amazon in turn adds the same key to the received string which then produces the original string corresponding to your credit card number (adding the key a second time "unlocks" the data).

To illustrate the idea, say you want to send an eight-digit binary string such as $s = 10101100$ to Amazon (actual credit-card numbers have very long strings) and Amazon sends your computer the key $k = 00111101$. Your computer returns the string $s + k = 10101100 + 00111101 = 10010001$ to Amazon, and Amazon adds k to this string to get $10010001 + 00111101 = 10101100$, which is the string representing your credit-card number. If someone intercepts the number $s + k = 10010001$ during transmission it is no value without knowing k . The method is secure because the key sent by Amazon is randomly generated and used only one time. You can tell when you are using an encryption scheme on a web transaction by looking to see if the web address begins with "https" rather than the customary "http." You will also see a small padlock in the status bar at the bottom of the browser window.

Application to Public Key Cryptography :-

In the mid-1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman devised an ingenious method that permits each person who is to receive a secret message to tell publicly how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message. The idea is based on the fact that there exist efficient methods for finding very large prime numbers (say about 100 digits long) and for multiplying large numbers, but no one knows an efficient algorithm for factoring large integers (say about 200 digits long). So, the person who is to receive the message chooses a pair of large primes p and q and chooses an integer r with $1 < r < m$, where $m = \text{lcm}(p - 1, q - 1)$, such that r is relatively prime to m (any such r will do). This person calculates $n = pq$ and announces that a message M is to be sent to him or her publicly as $M_r \bmod n$. Although r , n , and M_r are available to everyone, only the person who knows how to factor n as pq will be able to decipher the message. To present a simple example that nevertheless illustrates the principal features of the method, say we wish to send the message "YES." We convert the message into a string of digits by replacing A by 01, B by 02, . . . , Z by 26, and a blank by 00. So, the message YES becomes 250519. To keep the numbers involved from becoming too unwieldy, we send the message in blocks of four digits and fill in with blanks when needed. Thus, the message YES is represented by the two blocks 2505 and 1900. The person to whom the message is to be sent has picked two primes p and q , say $p = 37$ and $q = 73$ (in actual practice, p and q would have 100 or so digits), and a number r that has no prime divisors in common with $\text{lcm}(p - 1, q - 1) = 72$, say $r = 5$, and has published $n = 37 * 73 = 2701$ and $r = 5$ in a public directory. We will send the "scrambled" numbers $(2505)_5 \bmod 2701$ and $(1900)_5 \bmod 2701$ rather than 2505 and 1900, and the receiver will unscramble them. We show the work involved for us and the receiver only for the block 2505. The arithmetic involved in computing these numbers is simplified as follows:

$$2505 \bmod 2701 = 2505$$

$$(2505)^2 \bmod 2701 = 602$$

$$(2505)^4 \bmod 2701 = (602)(602) \bmod 2701 = 47$$

$$\text{So, } (2505)^5 \bmod 2701 = (2505)(47) \bmod 2701 = 2415.$$

Thus, the number 2415 is sent to the receiver. Now the receiver must take this number and convert it back to 2505. To do so, the receiver takes the two factors of 2701, $p = 37$ and $q = 73$, and calculates the least common multiple of $p - 1 = 36$ and $q - 1 = 72$, which is 72 (This is where the knowledge of p and q is necessary.) Next, the receiver must find $s = r^{-1}$ in $U(72)$ —that is, solve the equation $5 * s = 1 \bmod 72$. This number is 29. (There is a simple algorithm for finding this number.) Then the receiver takes the number received, 2415, and calculates $(2415)^{29} \bmod 2701$. This calculation can be simplified as follows:

$$2415 \bmod 2701 = 2415$$

$$(2415)^2 \bmod 2701 = 766$$

$$(2415)^4 \bmod 2701 = (766)^2 \bmod 2701 = 639$$

$$(2415)^8 \bmod 2701 = (639)^2 \bmod 2701 = 470$$

$$(2415)^{16} \bmod 2701 = (470)^2 \bmod 2701 = 2119$$

$$\text{So, } (2415)^{29} \bmod 2701 = (2415)^{16} (2415)^8 (2415)^4 \bmod 2701 =$$

$$(2119)(470)(639)(2415) \bmod 2701 = ((2119)(470) \bmod 2701 * (639)(2415) \bmod 2701) \bmod 2701$$

5(1962)(914) mod 2701 52505. [We compute the product (2119)(470)(639)(2415) in two stages so that we may use a hand calculator.]

Thus the receiver correctly determines the code for "YE." On the other hand, without knowing how pq factors, one cannot find the modulus (in our case, 72) that is needed to determine the intended message.

Digital Signatures :-

With so many financial transactions now taking place electronically, the problem of authenticity is paramount. How is a stockbroker to know that an electronic message she receives that tells her to sell one stock and buy another actually came from her client? The technique used in public key cryptography allows for digital signatures as well. Let us say that person A wants to send a secret message to person B in such a way that only B can decode the message and B will know that only A could have sent it. Abstractly, let E_A and D_A denote the algorithms that A uses for encryption and decryption, respectively, and let E_B and D_B denote the algorithms that B uses for encryption and decryption, respectively. Here we assume that E_A and E_B are available to the public, whereas D_A is known only to A and D_B is known only to B and that $D_B E_B$ and $E_A D_A$ applied to any message leaves the message unchanged. Then A sends a message M to B as $E_B(D_A(M))$ and B decodes the received message by applying the function $E_A D_B$ to it to obtain

$$(E_A D_B)(E_B(D_A(M))) = E_A(D_B E_B)(D_A(M)) = E_A(D_A(M)) = M.$$

Notice that only A can execute the first step [i.e., create $D_A(M)$] and only B can implement the last step (i.e., apply $E_A D_B$ to the received message).

Transactions using digital signatures became legally binding in the United States in October 2000.

Application to Genetics :-

The genetic code can be conveniently modeled using elements of $Z_4 \times Z_4 \times \dots \times Z_4$ where we omit the parentheses and the commas and just use strings of 0s, 1s, 2s, and 3s and add component wise modulo 4. A DNA molecule is composed of two long strands in the form of a double helix. Each strand is made up of strings of the four nitrogen bases adenine (A), thymine (T), guanine (G), and cytosine (C). Each base on one strand binds to a complementary base on the other strand. Adenine always is bound to thymine, and guanine always is bound to cytosine. To model this process, we identify A with 0, T with 2, G with 1, and C with 3. Thus, the DNA segment ACGTAACAGGA and its complement segment TGCATTGTCCT are denoted by

03120030110 and 21302212332. Noting that in Z_4 , $0 + 2 = 2$, $2 + 2 = 0$, $1 + 2 = 3$, and $3 + 2 = 1$, we see that adding 2 to elements of Z_4 interchanges 0 and 2 and 1 and 3. So, for any DNA segment $a_1 a_2 \dots a_n$ represented by element of $Z_4 \times Z_4 \times \dots \times Z_4$, we see that its complementary segment is represented by $a_1 a_2 \dots a_n + 22 \dots 2$.

Application to Electric Circuits :-

Many homes have light fixtures that are operated by a pair of switches. They are wired so that when either switch is thrown the light changes its status (from on to off or vice versa). Suppose the wiring is done so that the light is on when both switches are in the up position. We can conveniently think of the states of the two switches as being matched with the elements of $Z_2 \times Z_2$ with the two switches in the up position corresponding to (0, 0) and the two switches in the down position corresponding to (1, 1). Each time a switch is thrown, we add 1 to the corresponding component in the group $Z_2 \times Z_2$. We then see that the lights are on when the switches correspond to the elements of the subgroup $\{(1, 1)\}$ and are off when the switches correspond to the elements in the coset $(1, 0) + (1, 1)$. A similar analysis applies in the case of three switches with the subgroup $\{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$ corresponding to the lights-on situation

Conclusion:-

The role of external direct product in modern algebra cannot describe in a sentence. The use of external direct product is not only limited in group theory but also we can see the use of it in many branches of mathematics like topology and so on. If we come out from algebra then we can see that external direct product also plays a vital role in our daily life. So we can say a mathematics student should know the application of mathematics in daily life

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my advisor Prof. Peavanjan Kumar Rana , who introduced me to the wonderful project work . I would also like to thank him for the guidance , patience and help and for contributing from his abundance experience , knowledge and wisdom . It was an honour for me to get a glimpse to his world and way of thinking .My friend Sumit Paramanik and Agniva Bannerjee also helped me to do the project work , I am also thankful them.

References:-

1. John B. Fraleigh ,A first course of Abstract Algebra ,7th Ed.,pearson 2007
2. Joseph A. Gallian , Contemporary Abstract Algebra,4th Ed. Narosa Publishing House,1999
3. D.S.Malik,John M. Mordeson and M.K.Sen, Fundamental of Abstract Algebra

Project work
Submitted for partial fulfillment of the B.Sc. Degree
in Mathematics



*Under the supervision of **Dr. Pravanjan Kumar Rana***

By: -

Name: - Raj Das

Reg. No.-A01-1112-113-048-2019

Exam Roll No.-2022151126

Department of Mathematics

Ramakrishna Mission Vivekananda Centenary College

Rahara, Kolkata- 700118

ACKNOWLEDGEMENT

I would love reveal remarkable and extra special thanks to Dr. Pravanjan Kumar Rana, head of the department mathematics of RKMVCC Rahara, who gave me a very good opportunity to work on this project and with that his helpful behaviour helps me to complete this project.

I would also love to thank my group partners (Suman Parui and Soubhik Mandal) who helped me a lot on this project.

“Visual Interpretation of Sylow’s Theorem”

Key highlights: -

- *Introduction*
- *Sylow’s Theorem with visual interpretation*
- *Conclusion*
- *References*

INTRODUCTION

The **Sylow's theorems** are important tools in finite group theory. The **Lagrange's theorem** tells us that the order of a subgroup of a finite group is a divisor of the order of that group. The converse, however, is false. There are very few theorems which assert the existence of subgroups of prescribed order in arbitrary finite groups. The most basic and widely used, is a classic theorem due to the **Norwegian mathematician Sylow**.

There are three proofs of this result of Sylow. The **first** is a very elegant and elementary argument due to **Wielandt**. It appeared in the journal *Archiv der Mathematik*, vol. 10 (1959), pages 401-402. The basic elements in Wielandt's proof are number-theoretic and combinatorial. It has the advantage, aside from its elegance and simplicity, of producing the subgroup we are seeking. The **second** proof is based on an exploitation of induction in an interplay with the **class equation**. It is one of the standard classical proofs, and is a nice illustration of the combining many of the ideals developed so far to derive this very important cornerstone due to Sylow. The **third** proof is of a completely different philosophy. The basic idea there is to show that if a larger group than the one we are considering satisfies the conclusion of the Sylow's theorem, then our group also must. This forces us to prove Sylow's theorem for a special family of groups—the symmetric groups. By invoking Cayley's Theorem, we are then able to deduce Sylow's theorem for all finite groups. Apart from this strange approach—to prove something for a given group, first prove it for a much larger one—this third proof has its own advantages. Exploiting the ideas used, we easily derive the so-called **second and third parts** of Sylow's theorem. Here we discuss about the classical proof of Sylow's theorem with **visual interpretation**.

Sylow's Theorem with Visual Interpretation

If G is a Finite group of order n and if H is a subgroup of G , then we know by Lagrange's theorem that the order of H divides n . Sylow's Theorem gives the answer to the question, "If m is a positive integer, which divides n , does G contain a subgroup of order of m ?".

Definition:(p -groups, p -subgroups): A p -group is a group whose order is a power of a prime p , A p -group that is a subgroup of group G is called **p -subgroup** of G .

For example, D_4 is a 2-group, because its order is 8, a power of the prime 2.

Two important theorems about p -groups:

Theorem 1: If a p -group G acts on a set S , then the order of S and the number of stable elements in S are congruent mod p .

Theorem 2: If H is a p -subgroup of G , then $[N_G(H):H] \equiv_p [G:H]$

- **Sylow's First Theorem:** Let G be a finite group of order $p^r m$, where p is a prime, r and m are positive integers, and p and m are relatively prime. Then G has a subgroup of order p^k for all k , $0 \leq k \leq r$.

The First Sylow Theorem generalizes **Cauchy's Theorem** [If p is a prime number that divides $O(G)$, then G has an element g of order p , and therefore a subgroup $\langle g \rangle$ of order p .] in several ways, summarized in Table 1, its proof deals with both statements in the theorem at once by using Cauchy's Theorem to expand smaller p -subgroup to create larger ones. The First Sylow tells us a bit about the relationship among p -subgroups, but we will learn more about that relationship from Second Sylow Theorem.

Proof.

It is easy to find a p -subgroup of order 1 (which is p^0) because it is obviously

Cauchy's Theorem	First Sylow Theorem
If p divides $O(G)$, then there is a subgroup of order p .	If p^i divides $o(G)$, then there is a subgroup of order p^i .

<i>It is cyclic and has no subgroups.</i>	<i>Each has subgroups of orders 1, p, p^2, up to p^i.</i>
<i>There is also an element of order p.</i>	<i>There is not necessarily an element of order p^i.</i>

$\{e\}$. We also know that there is a p -subgroup of order p (which is p^1) from Cauchy's Theorem (as long as $O(G) > 1$). The main job of this proof is showing the existence of the larger subgroups, by explaining how to make any $H < G$ of any order $p^i < p^n$ and expand it to create a new subgroup $H^* < G$ that contains H and is p times as large, as shown in the given figure. We can then repeatedly expand the smallest p -subgroups, creating larger ones up to size p^n .

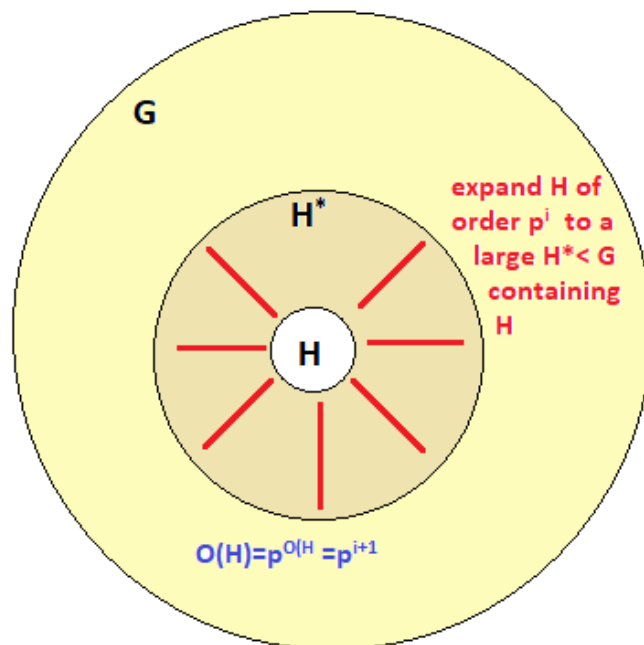


Figure: First Sylow Theorem gives a procedure for taking a subgroup of order p^i and finding a larger subgroup whose order is p^{i+1} (as long as p^{i+1} divides $O(G)$).

We can find the H^* we seek inside the normalizer $N_G(H)$ by relying on the fact that $H \triangleleft N_G(H)$. Next figure illustrates the groups, subgroups, and homomorphism that come into play in the rest of this proof; refer to it help **visualize** the following argument. Create the quotient group $N_G(H)/H$ and call the quotient map q . The size of the quotient group is the number of cosets of H in its normalizer, $[N_G(H):H]$, which Theorem 2 says must be congruent to $[G:H] \pmod{p}$. So, what do we know about $[G:H]$? We're given that the order of G is some multiple of p^n , say $p^n m$. So, the number of cosets of H is

$$[G:H] = O(G)/O(H) = p^n m / p^i = p^{n-i} m.$$

Because $p^i < p^n$, we know that $p^{n-i} > 1$ and so p divides $p^{n-i} m$. Therefore $[G:H]$ and $[N_G(H):H]$ are both multiples of p .

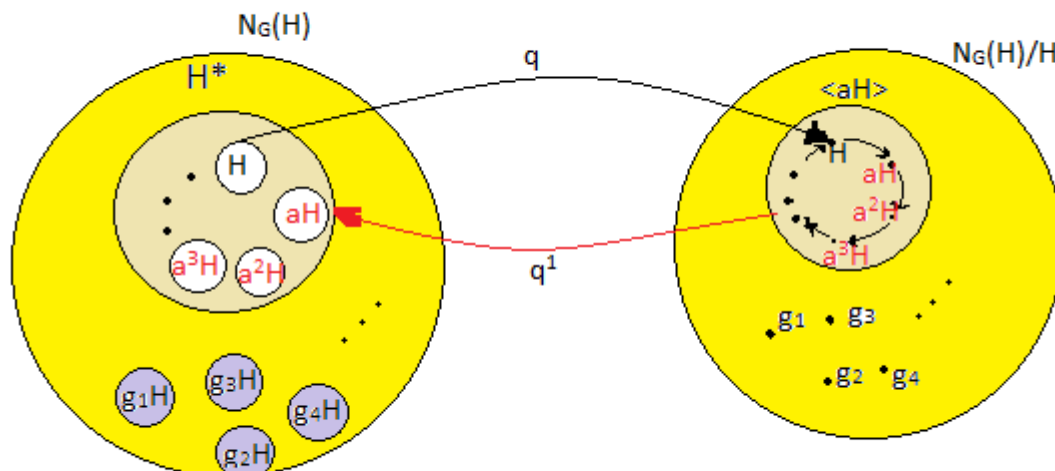


Figure: The quotient map and its inverse used in First Sylow theorem to create a subgroup H^* whose order is p times of H

The order of $N_G(H) / H$ is obviously not 0, so it must be a positive multiple of p . This lets us use Cauchy's theorem to find an element of order p in the quotient group; call that element aH . The cyclic subgroup $\langle aH \rangle$ will be very useful to us. The collection of elements that q maps to $\langle aH \rangle$ obviously contains H , but as above Figure suggests it is also a subgroup of $N_G(H)$. It is the subgroup H^* that we seek; it contains H and has size p^{i+1} for the following reason. There are p elements in $\langle aH \rangle$, and therefore p cosets of H in H^* . Since H contains p^i elements, each of its cosets does as well, and H^* contains p of them, for a total of p^{i+1} elements. The preceding paragraphs give a way to expand any H of order $p^i < p^n$ into a larger H^* of order p^{i+1} . Beginning with $H = \{e\}$, we can repeatedly expand it to create H^* , H^{**} , and so on of orders p , p^2 , up to p^n .

The expansion technique in this proof is an example of conjugacy. It applies q to H , applies Cauchy's theorem in the quotient group to turn one element into p elements, and applies q^{-1} to bring those p elements back into G , as p cosets

forming a subgroup H^* . Even though q^{-1} isn't really a function, this is a useful way to summarize the argument.

Now we discuss Second and third part of Sylow's Theorem shortly:

- **The Second Sylow Theorem: Relationship among p -subgroups:**

The First Sylow Theorem guarantees the existence of subgroups of certain sizes, and what it told us of the relationship among such groups was that all smaller p -subgroups are inside larger ones. The Second Sylow Theorem shows us how the largest such p -subgroups relate through conjugacy.

Definition: (Sylow p -subgroup): We call H a Sylow p -subgroup of G if it is a p -subgroup whose order is the highest power of p that divides $O(G)$. In other words, H is a p -subgroup of G that's either the largest one, or tied for it.

Theorem:(Sylow's Second Theorem): Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then any two Sylow's p -subgroups of G are **conjugate**, and therefore **isomorphic**.

Here we mention some of its important consequences that may not at first be obvious. Conjugating by any group element creates an isomorphism from the group to itself called an inner automorphism. Thus, when two subgroups are conjugates (say $H = gKg^{-1}$), there is an inner automorphism mapping one to the other ($\Phi(x) = gxg^{-1}$). Therefore, conjugate subgroups are isomorphic. The Second Sylow Theorem tells us that all of a group's largest p -subgroups are one another's conjugates, and so they are all isomorphic to one another. Now recall the nesting relationship among p -subgroups given by the First Sylow Theorem, so that every p -subgroup is inside a Sylow p -subgroup. Conjugating any Sylow p -subgroup by any group element results in a (possibly different) Sylow p -subgroup, with identical internal structure, as shown in the Figure.

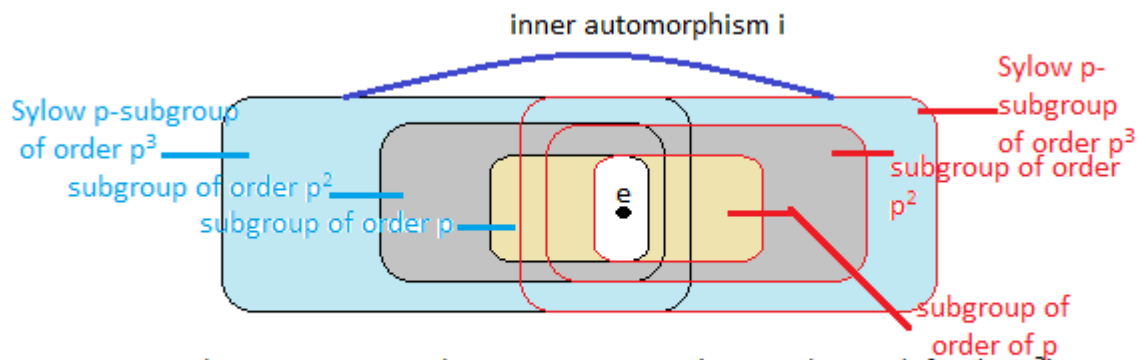


Figure: The inner automorphism i maps one Sylow p -subgroup (of order p^3) to another, which therefore has identical internal structure.

Therefore, any smaller p -subgroup must have a copy of itself (one of its conjugates) in every Sylow p -subgroup.

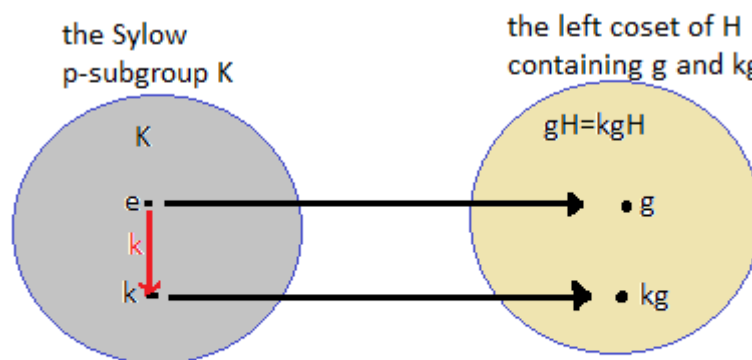


Figure: A stable element gH of the group action in the proof of the Second Sylow Theorem is one for which, for any k belong to K , $kgH = gH$.

it appears to intersect the original Sylow 2-subgroup only at the identity, that is just one possibility. For instance, if $\langle a \rangle$ were a normal subgroup, then it would be conjugate only to itself, so every Sylow 2-subgroup would contain all of $\langle a \rangle$.

- **Sylow's Third Theorem: Number of p -subgroups:**

Let G be a finite group of order $p^r m$, where p is prime, r and m are positive integers, and p and m are relatively prime. Then the number n_p of Sylow p Subgroups of G is $1 + kp$ for some nonnegative integer k and $n_p \mid p^r m$

This theorem helps us narrow down, just based on a group's order, the possible number of Sylow p -subgroups that the group can have.

Conclusion

The Sylow's Theorems are a powerful statement about the structure of groups in general, but are also powerful in applications of finite group theory.

Sometimes we need visualize concepts to understand the topic deeply. First, we introduce p -groups, some necessary Theorems. Then gives statement of Sylow's theorems and proof all of them with visualization. That's all from our project work.

References

- *Visual Group Theory* by Nathan C. Carter, Bentley University.
- *Topics In Algebra* by I. N. Herstein, University of Chicago.
- *Fundamentals of Abstract Algebra*, D.S. Malik (Creighton University), John M. Mordeson (Creighton University), M.K. Sen (Calcutta University).

College Name: Ramakrishna Mission Vivekananda Centenary College

Name: Sreyan Jha

Reg. No: A01-1112-113-020-2019

Exam Roll No: 2022151107

College Roll No: 330

Project Topic: Todd-Coxeter Algorithm

Supervised by: Pravanjan Kumar Rana

Acknowledgement

I would like to express my special thanks of gratitude to my advisor, Prof. Pravanjan Kumar Rana, who introduced me to the wonderful project work. I would also like to thank him for the guidance, patience, and help and for contributing from his abundance experience, knowledge and wisdom. It was an honour for me to get a glimpse to his world and way of thinking. My friends Anischay Pal and Partha Das also helped me to do this project work, I am also thankful to them.

CONTENT

<u>SI No.</u>	<u>Subject</u>	<u>Page No.</u>
01.	Introduction	4
02.	Todd-Coxeter Algorithm	4-6
03.	Example	7-13
04.	Implementation	13-15
05.	Application	15-16
06.	Conclusion	17
07.	References	17

Introduction:

In group theory, the **Todd–Coxeter algorithm**, created by J. A. Todd and H. S. M. Coxeter in 1936, is an algorithm for solving the coset enumeration problem. Let G be a group described by a finite presentation, and let H be a subgroup described by a generating set. Then the Todd-Coxeter algorithm is a strategy for writing down the set of left cosets of H in G together with the action of G on the set.

Todd–Coxeter Algorithm:

Let G be the finitely presented group

$$G := \langle g_1, g_2, \dots, g_n \mid r_1(g_1, g_1, g_2, \dots, g_n) = e, \dots, r_m(g_1, g_1, g_2, \dots, g_n) = e \rangle$$

or shorter $G := \langle E \mid R \rangle$ where $E := \{g_1, g_2, \dots, g_n\}$ and $R := \{r_i(g_1, g_1, g_2, \dots, g_n) \mid i = 1, 2, \dots, m\}$ where each relator $r_i(g_1, g_1, g_2, \dots, g_n)$ is a word in g_1, g_2, \dots, g_n and e is the identity of G , and let H be the subgroup of G generated by the set S of words,

$$S := \{s_1(g_1, g_1, g_2, \dots, g_n), \dots, s_p(g_1, g_1, g_2, \dots, g_n)\}$$

that is, $H := \langle S \rangle$.

The algorithm is based on two simple facts:

1. If $s \in S$, then $Hs = H$.
2. If $r(g_1, \dots, g_n)$ is a relator, then for any coset Hx , $x \in G$ we have $Hxr(g_1, \dots, g_n) = Hx$. So if $r(g_1, \dots, g_n) = g_{i1} \dots g_{it}$ where each g_{ij} is a generator or an

inverse of a generator, then: $H_0 := Hx$, $H_1 := H_{0g_{i1}}$, $H_2 := H_{1g_{i2}}$, \dots , $H_j := H_{j-1g_{ij}}$ is defined, then $H_t = H_0$.

Now, for the procedure itself: for each word that generates the subgroup H we maintain a one-line table, called a subgroup table. The row is labelled as 1 for the coset H itself. The columns are labelled by the factors of the generator of the word. That is, if $s_j = g_{i1} \dots g_{ik}$ is a generator of H , then we have $k + 1$ columns.

Subgroup Table

<u>g_{i1}</u>	<u>g_{i2}</u>	<u>\dots</u>	<u>g_{ik}</u>
1			1

If we look at the table as a matrix of order $1 \times (k + 1)$, then the entry $(1, g_{ij})$ in the table, if defined, is the number of the coset we get from the multiplication $1 \cdot g_{i1} \dots g_{ij}$.

For each relator, $r (g_1, \dots, g_n)$ we have a relation table. Relation tables will give us information in case two cosets which have numbered differently are the same. If a relation acts on two cosets in exactly the same way, then these cosets must be identical. The rows of the relation tables are labelled with the numbering we defined for the cosets. Similarly to the subgroup table, given a relator $r_i = g_{i1} \dots g_{ik}$, we have $k + 1$ columns.

Relation table for $r_i = g_{i1} \dots g_{ik}$

<u>$g_{i1}g_{i2} \dots g_{ik}$</u>		
	1	1
	2	2
	.	.
	.	.
	.	.
	t	t
	.	.
	.	.

As in the subgroup table, the entry (n, g_{ij}) if defined, is the coset we get from the multiplication $n \cdot g_{i1} \cdot g_{i2} \cdots g_{ij}$. Since we know that $r_i = g_{i1} \cdots g_{ik} = e$, we get that $Hxr_i = Hx$. So the entry (n, g_{ik}) is n .

Finally, we would like to have a table that keeps track for us on the result of multiplications. This table is the coset table. The rows will be labelled with the numbers of the cosets, and the columns will be labelled by the generators of G and their inverses (unless a generator is an involution). The entry (n, g_i) , if defined, is $n \cdot g_i$ for the coset n and the generator g_i .

When the last entry in a row of a relation table or a subgroup table is filled in, we get an extra piece of information, in the form of $n \cdot g = l$, for some cosets n, l and a generator g . This extra piece of information is called a deduction. When getting a deduction we can face three situations:

- (i) The entries (n, g) and (l, g^{-1}) are still empty. In this case, we just fill the number l in the entry (n, g) and the number n in the entry (l, g^{-1}) . We also insert this information into all other relevant places in the other tables.
- (ii) The entry (n, g) is already filled with the number l . In this case, the deduction brings no new information.
- (iii) At least one of the entries (n, g) or (l, g^{-1}) in the coset tables is filled with a number different from l or n , respectively. In this case, we conclude that we have two different numbers to the same coset. This phenomenon is called a coincidence. When a coincidence is found, we replace both numbers by the smaller one in all places they occur.

The process terminates when all the entries of the coset, relation and subgroup tables are filled.

We would like to give a detailed example of the Todd-Coxeter Algorithm for the group S_4 , using generators and relations, as follows:

$G := \langle a, b, c \mid a^2 = b^2 = c^2 = e, (ab)^3 = e, (bc)^3 = e, (ac)^2 = e \rangle$

and taking the subgroup

$H := \langle a, b \rangle$.

We have to use some useful proposition

- (i) The set of transpositions $\{(1, k) \mid 1 \leq k \leq n\}$ generate S_n , for $n \geq 2$
- (ii) The set of transpositions $\{(12), (23), \dots, (n-1, n)\}$ generate S_n , for $n \geq 2$.

First, we define three cosets and try to fill in the tables. Then we will be able to see whether we need to define more cosets in order to complete the tables, or not.

We define:

$1 := H, 2 := 1c, 3 := 2b$.

The subgroup tables are already closed, and as expected, we did not gain any additional information from them.

Subgroup Tables

<u>a</u>		<u>b</u>	
1	1	1	1

However, from the definitions and the relations in the group G , we can immediately derive the following: $2c = 1$, $3b = 2$, as b and c are of order 2. We should note that there are a few possible ways to fill in the tables. One can start from the left or from the right and then can continue using any combination of them. Nevertheless, eventually one arrives at the same result.

Now, let us start filling in the coset and relation tables:

Coset table

	a	b	c
1	1	1	2
2	2	3	1
3		2	3

Relation tables for $a^2 = e$, $b^2 = e$, $c^2 = e$

<u> a a </u>			<u> b b </u>			<u> c c </u>		
1	1	1	1	1	1	1	2	1
2	2	2	2	3	2	2	1	2
3		3	3	2	3	3	3	3

Relation table for $(ab)^3 = e$

	<u> a b a b a b </u>
1	1 1 1 1 1 1 1
2	2 2 3 3 2
3	3 2 2 3

Relation table for $(ac)^2 = e$

	a	c	a	c
1	1	<u>2</u>	<u>2</u>	1
2	2	1	1	2
3	3		3	3

Relation table for $(bc)^3 = e$

b	c	b	c	b	c	
1	1	2	3	3	2	1
2	<u>3</u>	<u>3</u>	2	1	1	2
3	2	1	1	2	3	3

In the process of filling in the tables we have received the following deductions, $2a = 2$, $3c = 3$, which we have underlined in the table, in the place we got them.

Now, one can define one more coset and continue, or to define a few more at once. As we shall see, it is enough to define only one more coset, namely, $4 := 3a$ to complete all the tables. However, since we would like to demonstrate the notion of "coincidences" we shall take the latter approach: we shall define three more cosets at once: $4 := 3a$, $5 := 4b$, $6 := 4c$. Continuing filling in the tables gives

	a	b	a	b	a	b
1	1	1	1	1	1	1
2	2	3	<u>4*</u>	<u>4*</u>	3	2
3	4	<u>5*</u>	<u>3*</u>	2	2	3
4	3	2	2	3	5	4
5	3	2	2	3	4	5
6	3	2	2	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 ₅	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we receive the following deductions: $4b = 4$ and $5a = 3$. However, as we see in the coset table, the place of $4b$ is already filled with 5. Therefore, we get a coincidence: cosets 4 and 5 are the same coset of H in the group G . Similarly, the place of $3a$ is already filled with 4 in the coset table, which means, as have already discovered, that 4 and 5 are the same coset. We note that coincidences are marked in the tables with asterisk(*). Equipped with the previous information, let us continue to the other relation tables.

	a	c	a	c
1	1	2	2	1
2	2	1	1	2
3	4	<u>6*</u>	<u>3*</u>	3
4	3	3	4	4
5	3	3	4	5
6	3	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4 _{5,6}	2	3
4	3	5 ₄	6
5	3	4	
6	3		4

From this relation table we get the information that $6a = 3$ or, equivalently, $3a = 6$. This yields another coincidence: this time we get that cosets 4 and 6 are the same cosets of H in G . So, from the last two coincidences we have $4 = 5 = 6$. These coincidences yield full information about the multiplication of all the elements we have, or in other words, we filled in the whole coset table, and thus can fill in the rest of the tables completely. As we said in the description of the algorithm, we take the smallest integer in a coincidence to represent the equal cosets.

	a	b	c
1	1	1	2
2	2	3	1
3	$4_{5,6}$	2	3
4	3	5_4	6_4
5	3	4	4
6	3	4	4

	a			b			c	
1	1	1	1	1	1	1	2	1
2	2	2	2	3	2	2	1	2
3	4	3	3	2	3	3	3	3
4	3	4	4	5	4	4	6	4
5	3	5	5	4	5	5	4	5
6	3	6	6	4	6	6	4	6

	b	c	b	c	b	c
1	1	2	3	3	2	1
2	3	3	2	1	1	2
3	2	1	1	2	3	3
4	4	4	4	4	4	4
5	4	4	4	4	4	5
6	4	4	4	4	4	6

Eventually, we receive four different cosets of H in G , which are 1,2,3 and 4. This means that $[G : H] = 4$, and since $|H| \leq 6$ then we get an upper bound to the order of G , that is, $|G| \leq 24$. On the other hand, we know that the three transpositions (12),(23),(34), of which the generators of G act on the cosets 1,2,3 and 4, generate S_4 and we get an epimorphism from G onto S_4 (or equivalently, S_4 is a homomorphic image of G), which means that $|G| \geq 24$. All in all, we get that $|G| = 24$ and thus $G \cong S_4$.

Implementation

Now we give a concrete implementation of the algorithm in Python. For simplicity, we will just compute $S_3/\langle b \rangle$ with the presentation $\langle a, b | a^3, b^2, abab \rangle$

The main data structures are

```
idents = []

neighbors = []
to_visit = 0

ngens = 2
rels = [
    (1, 0), # a^-1a
    (3, 2), # b^-1b
    (0, 0, 0), # a^3
    (2, 2), # b^2
    (0, 2, 0, 2) # abab
]
hgens = [
    (2,), # b
]

def find(c):
    c2 = idents[c]
    if c == c2:
        return c
    else:
        c2 = find(c2)
        idents[c] = c2
        return c2

def new():
```

```

    c = len(idents)
    idents.append(c)
    neighbors.append((2*ngens)*[None])
    return c

def unify(c1, c2):
    c1 = find(c1)
    c2 = find(c2)
    if c1 == c2:
        return
    c1, c2 = min(c1, c2), max(c1, c2)
    idents[c2] = c1
    for d in range(2*ngens):
        n1 = neighbors[c1][d]
        n2 = neighbors[c2][d]
        if n1 == None:
            neighbors[c1][d] = n2
        elif n2 != None:
            unify(n1, n2)

def follow(c, d):
    c = find(c)
    ns = neighbors[c]
    if ns[d] == None:
        ns[d] = new()
    return find(ns[d])

def followp(c, ds):
    c = find(c)
    for d in reversed(ds):
        c = follow(c, d)
    return c

start = new()

for hgen in hgens:
    unify(followp(start, hgen), start)

while to_visit < len(idents):
    c = find(to_visit)
    if c == to_visit:
        for rel in rels:
            unify(followp(c, rel), c)
    to_visit += 1

print ("done")

cosets = [c for i, c in enumerate(idents) if i == c]

```

```
perms = [[cosets.index(follow(c, 2*d)) for i, c in enumerate(cosets)]
          for d in range(ngens)]

def cycle(perm):
    parts = []
    for i in range(len(perm)):
        part = [str(i+1)]
        k = perm[i]
        while k != i:
            if k < i: break
            part.append(str(k+1))
            k = perm[k]
        else:
            parts.append(" ".join(part))
    return "("+" ".join(parts)+")"
for d in range(ngens):
    print ("g%d =" %d, cycle(perms[d]))
```

For these particular relations, the output is

```
done
g0 = (1 2 3)
g1 = (1) (2 3)
```

Application:

By using this algorithm, Coxeter and Todd showed that certain systems of relations between generators of known groups are complete, that is constitute systems of defining relations. If the order of a group G is relatively small and the subgroup H is known to be uncomplicated, then the algorithm can be carried out by hand and gives a reasonable description of the group G . It is a systematic procedure for enumerating the cosets of a subgroup of finite index in a group given by generators and relations. The algorithm has been an important component in most

computer programs to date dealing with symbolic calculation in algebra.

We use programmes for the Todd-Coxeter coset enumeration algorithm and the modified Todd-Coxeter coset enumeration algorithm to investigate a class of generalised Fibonacci groups. In particular we use these techniques to discover a finite non-metacyclic Fibonacci group.

There are a number of things one can deduce from the result of the algorithm.

- Of course, if it terminates, we deduce $[G:H]$ is finite (and know what it equals).
- A permutation representation of G/H , given by a permutation of G/H for each generator of G .
- Whether H is a normal subgroup. This can be determined by seeing whether each generator's permutation is an element of $\text{Aut}(G/H)$, since then $\text{Aut}(G/H) = G/H$, implying H is normal.
- An algorithm for the word problem for the group. Given two words, follow the graph from the basepoint to see whether they end on the same vertex.
- The algorithm also helps to compute the data of a uniform polytope.

Conclusion:

The Todd–Coxeter algorithm can be applied to infinite groups and is known to terminate in a finite number of steps, provided that the index of H in G is finite. On the other hand, for a general pair consisting of a group presentation and a subgroup, its running time is not bounded by any computable function of the index of the subgroup and the size of the input data.

References:

- .Brown, Ken. *The Todd-Coxeter procedure*.
- Coxeter, H. S. M.; Moser, W. O. J. (1980). *Generators and Relations for Discrete Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 14 (4th ed.). Springer-Verlag 1980. ISBN 3-540-09212-9. MR 0562913.
- Seress, Ákos (1997). "An introduction to computational group theory" (PDF). Notices of the American Mathematical Society. 44 (6): 671–679. MR 1452069.



GEOMETRICAL APPROACH ON CLASS EQUATION IN GROUP THEORY

PROJECT WORK

Prepared by

Siddhartha Chakraborty

Registration no: A01-1112-113-023-2019

Examination roll no. 2022151110

Under the supervision of Dr. Pravanjan Kumar Rana

Department of Mathematics

RAMAKRISHNA MISSION VIVEKANANDA CENTENARY COLLEGE, RAHARA,
KOLKATA -700118

ACKNOWLEDGEMENT

Presentation inspiration and motivation have always played a key role in the success of my adventure.

We would like to express our special thanks of gratitude to our respected teacher Dr.P.K.Rana,H.OD. of Mathematics, Ramakrishna Mission Vivekananda Centenary College, Rahara, who gave us the golden opportunity to do this wonderful project on the topic “Geometrical Approach on Class Equation in Group Theory” which also helped me in doing a lot of research and I come to know about so many new things.

We would also like to extend our gratitude to the principle Sir Swami Kamalasthananda and Vice principle Swami Vedanuragananda for providing me with the facility that was required.

Secondly, we would also like to thank our friends who helped us a lot to finish this project within the limited time.

Last, but not the least, our parents are also an important inspiration for us so with due regards, we express our gratitude to them.

It helped us to increase our knowledge and skills.

Siddhartha Chakraborty

Date :13/01/2022

ABSTRACT: In mathematics, group theory plays a great role. Here I would like to discuss about the geometrical approach on class equation of group theory. Before dive into the topic, we see a quick overview of trough out the topic, that is see some definitions, lemmas, theorems, then entre into the main topic and at last I shall try to create a 3-D model for class equation of group. Now let's starts the journey.

INTRODUCTION: To develop my project, I need some basic definitions, some theorems, lemmas, etc. Here it is.

- A relation between nonempty sets X and Y is a subset $R \subseteq X \times Y$. We say that $x \in X$ is related to $y \in Y$ if $(x, y) \in R$. If that be the case, we shall denote it by xRy .
- Let, X be a nonempty set. A relation \sim on X is said to be an equivalence relation if it is reflexive, symmetric, transitive.

Thus, a relation \sim on X is an equivalence relation if for every $x, y, z \in X$
 (i) $x \sim x$, (ii) $x \sim y$ implies $y \sim x$ and (iii) $(x \sim y)$ and $(y \sim z)$ implies $x \sim z$.

- Suppose \sim is an equivalence relation on a nonempty set X . For $x \in X$ define $[x] := \{y \in X : x \sim y\}$

The subset $[x]$ of X is called the equivalence class of x for \sim . It is the collection of all those elements in X which are related to x for the relation \sim .

- **Lemma:** Let X be a nonempty set and \sim be an equivalence relation on X . If $y \in [x]$, then $[x] = [y]$.
- **Theorem:** Let X be a nonempty set and an equivalence relation on X . Let $x, y \in X$. Then exactly one of the following is true.
 - (i) $[x] \cap [y] = \emptyset$.
 - (ii) $[x] = [y]$.
- A partition of a nonempty set X in a pairwise disjoint collection of subsets of X whose union is X .
- Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab . We say G is a group under this operation if the following three properties are satisfied.
 1. Associativity. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G .
 2. Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G .
 3. Inverses. For each element a in G , there is an element b in G (called an inverse of a) such that $ab = ba = e$.
- The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G . In symbols, $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}$.

So, now let's start the main discussion.

Let, G is a group. Then, G is a set, it is obvious. We consider a relation " R " on that set G such that $g R h \Leftrightarrow xgx^{-1}=h$, for some $x \in G$ and $g, h \in G$.

First, we have to show " R " is an equivalence relation.

- I. Let, e_G is the identity element of a group G , then for all $a \in G$ we have $e_G * a * e_G^{-1} = a$. that is $a R a$ implies " R " is a 'reflexive relation'.
- II. Let, $g, h \in G$ and $g R h$, then for some $x \in G$, we have, $x * g * x^{-1} = h$
or, $x^{-1} * (x * g * x) * x = x^{-1} * h * x$
or, $g = x^{-1} * h * x = (x^{-1}) * h * ((x^{-1})^{-1})$
or, $h R g$ [since, $x \in G$ (group), then $x^{-1} \in G$]

Then " R " is a 'symmetric relation'.

- III. Let, $f, g, h \in G$ and $f R h$, $g R h$, then $x * f * x^{-1} = g$ and, $y * g * y^{-1} = h$, hence $y(x * f * x^{-1}) * y^{-1} = h$

Or, $f R h$, so " R " is a 'transitive relation'.

Then " R " is an "**equivalence relation**" (also known as **conjugacy relation**) on the set G (group).

Let, $a \in G$ then the *equivalence class* (also called *conjugacy class*) of that set G corresponding to that element " a " is the set $\{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$ and also denoted as $CL(a)$ or, $[a]$, that is $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \text{ for some } x \text{ in } G\}$.

[we already know that the followings are hold, that is 1. $[g_1] = [g_2]$ or, 2. $[g_1] \cap [g_2] = \emptyset$. Where g_1, g_2 are two elements in G then one of them is hold]

Now we have, $G = \cup [a_i]$ (1)

Note that: Let, a in G such that a in $Z(G)$, then $[a] := \{g \text{ in } G \mid g = x * a * x^{-1}, \forall x \in G\}$
 $= \{g \in G \mid g = a\}$
 $= \{a\}$

Now, if, $[a] = \{a\}$, then, $g = x * a * x^{-1}, \forall x \in G$
or, $a = x * a * x^{-1}, \forall x \in G$
or, $a * x = x * a, \forall x \in G$

hence, $a \in Z(G)$, where $Z(G)$ is the center of the group G .

Now we have the result $[a] = \{a\} \Leftrightarrow a \in Z(G)$.

Or, $a \in CL(a) \Leftrightarrow a \in Z(G)$.

Note that: $Z(G) \cap [a] = \emptyset$

Now, equation (1) implies $G = Z(G) \cup CL(a_1) \cup \dots \cup CL(a_n)$, where, $o(Z(G)) = m$, i.e. for all g_i in $Z(G)$, we have $[g_i] = \{g_i\}$, $m+n = k$.

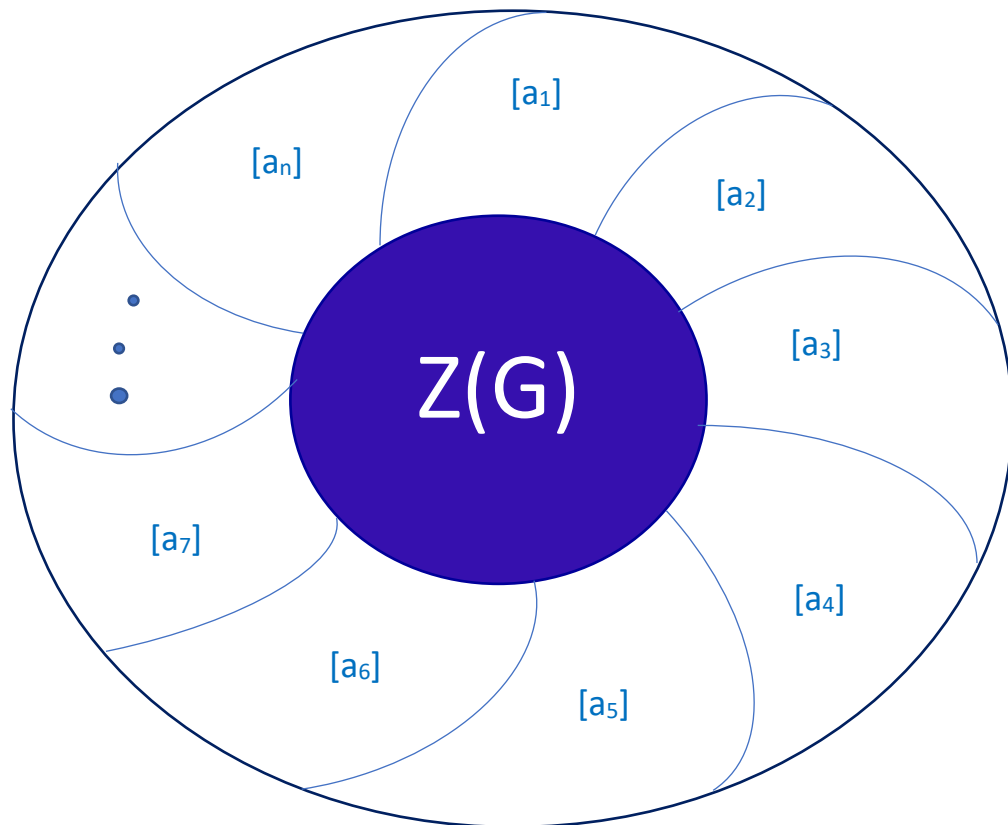
So, $O(G) = O[Z(G)] + \sum_{i=1}^n [a_i]$ (2)

Equation (2) is called the '*class equation of a finite group*'.

The class equation of a finite group can also be written as $|G|=|Z(G)|+\sum_{i=1}^n [G:C(a_i)]$.

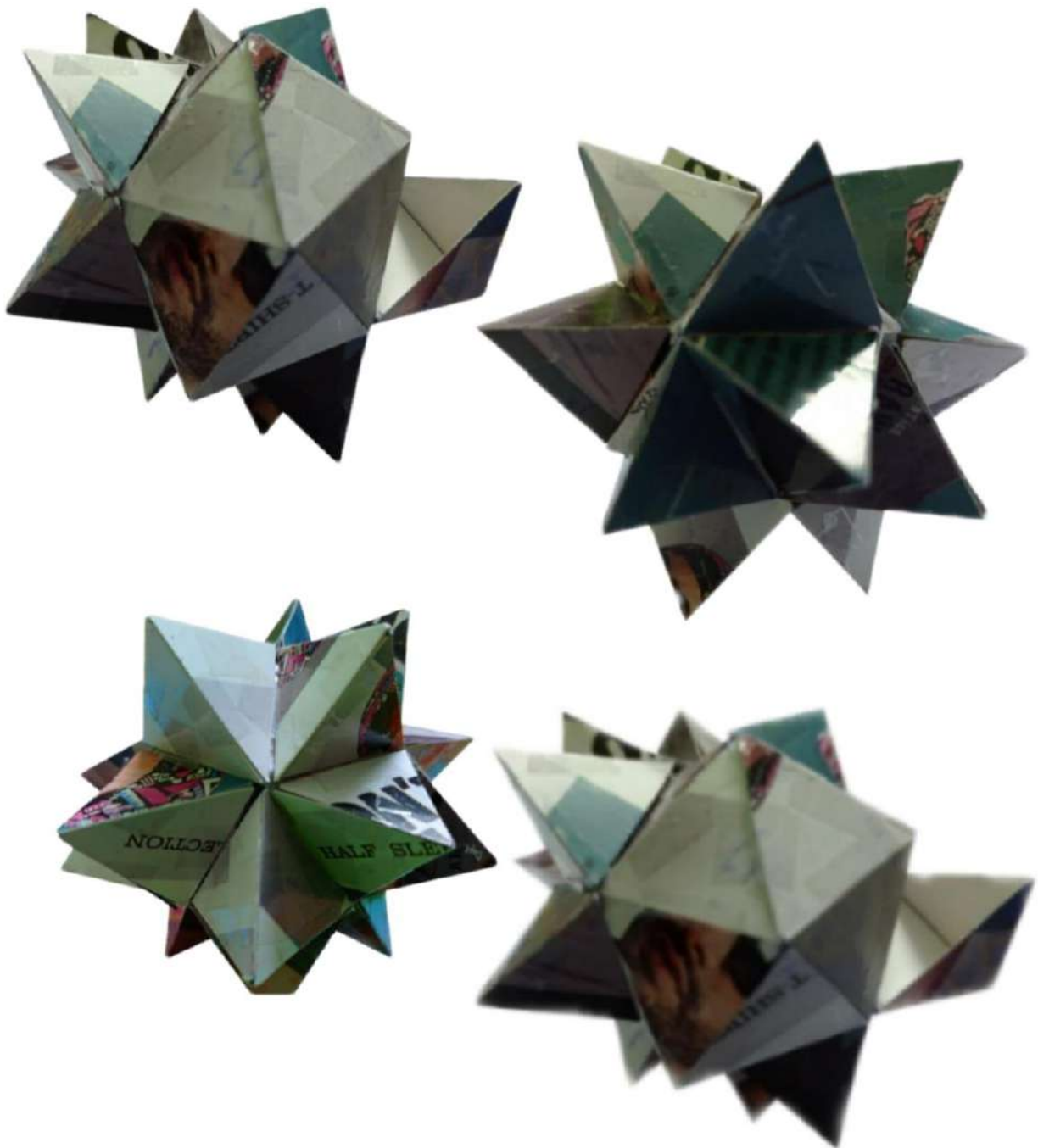
Here I try to create a diagram(2-D) of the class equation of the finite group G .

Here we try to create a diagram of the class equation of the finite group G .



[Partition of group G]

We are trying to set up a higher dimensional model for CLASS EQUATION of a GROUP(G).



REFERENCE BOOKS:

S. K. Mapa, Higher Algebra (Classical, Abstract & Linear).

M. K. Sen, S. Ghosh, P. Mukhopadhyay, Topics in Abstract Algebra.

Joseph A. Gallian, Contemporary Abstract Algebra, 4th Ed., Narosa Publishing House, New Delhi, 1999

CONCLUSION: I enjoyed this project very much, because in that field of mathematics there are so many abstract concepts, and also heart touching experiences, there are no end points of abstract algebra, since I believe that so many beautiful things also be found in future.

RKMVCC RAHARA

Department of Mathematics

Semester: 5th

Core Course-XII

Group Theory-II

Project member:

Aniket Chakraborty

Exam Roll-2022151123

Reg No.-A01-1112-113-044-2019

Supervised by:

Dr. Pravanjan Kumar Rana

ACKNOWLEDGEMENT

I would like to express special thanks and my special gratitude to **Dr. Prabanjan kumar Rana, head of the department mathematics of RKMVCC Rahara**, who gave me a golden opportunity to do this project and also provided support in completing my project work.

I would also like to extend my gratitude to my friend Ritoprovo Roy, who helped me by sketching the drawings for my project.

TOPIC

Geometry of Orbits in Three Dimensional Sphere

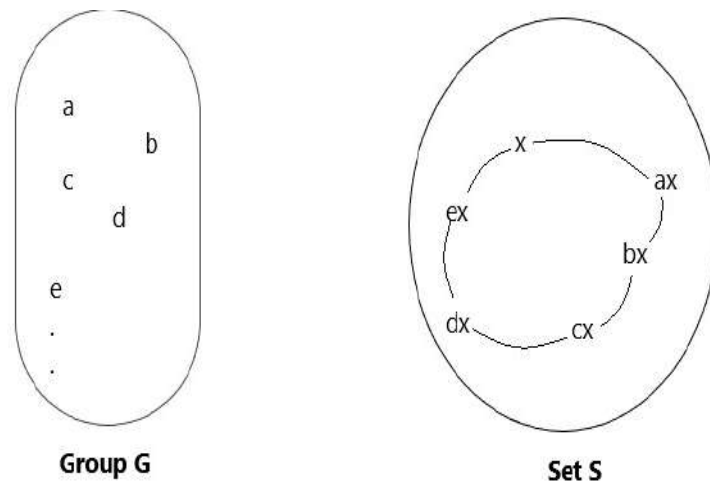
1. Abstract:

In this context we discussed geometry of orbits in light of three dimensional systems especially in a Sphere. Here we consider the group G as $(\mathbb{R}, +)$ and the set S as \mathbb{R}^2 . When S is a G set, we denote the group action by $\varphi: G \times S \rightarrow S$. Here the orbits orient themselves as a plane in three dimensional geometry containing three axes "X", "Y" & "Z" .

2. Introduction:

Let, G be any group whose elements are of the form $\{a, b, c, d, \dots e\}$. Also let S be a nonempty set & $x \in S$.

Keeping the element x fixed, we take all the elements of the form gx where $g \in G$ from the set S .



The set that contains elements of the form gx where $g \in G$, where x is a fixed element, is called the Orbit of x .

2.1 Definition of orbit:

Let, G be a group, acting on a non-empty set S . If $x \in S$, then the trajectory $\{\varphi(g, x): g \in G\}$ of the point x is called the orbit of the point x . It is denoted by O_x or by $[x]$.

2.2. Definition respect to equivalence relation:

Let, G be a group, acting on a non-empty set S . Now we define a relation ' \sim ' on S by $a \sim b \Leftrightarrow ga = b$ for some $g \in G$ & $\forall a, b \in S$. Then the relation ' \sim ' is an equivalence relation.

- The equivalence classes determined by the equivalence relation ' \sim ' are called the Orbits of G on S .

3. Concept of geometry of orbits:

For ease of understanding we can imagine the universe as a group. Then we can observe that every planet has own Orbit. We have the orbits never intersects with each other and they follow their own path. Each and every orbit has their different pattern of different shapes. We will discuss this in this context.

EXAMPLE-3.1: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x + t, y) \forall t \in G \ (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

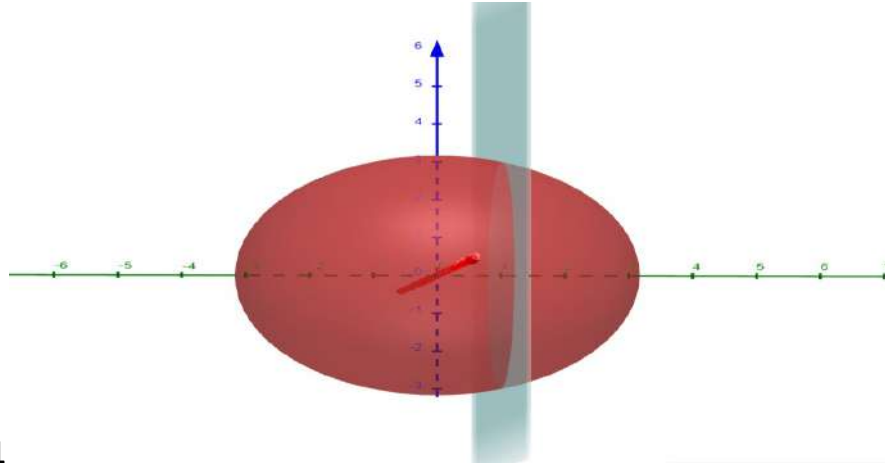
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), 1: t \in \mathbb{R}\}$$

$$\{(x, 1): x \in \mathbb{R}\}; \text{ where } (1 + t) = x$$

For this case the Y coordinate is always 1

i.e. horizontal line parallel to X axis, above the origin



Picture-1

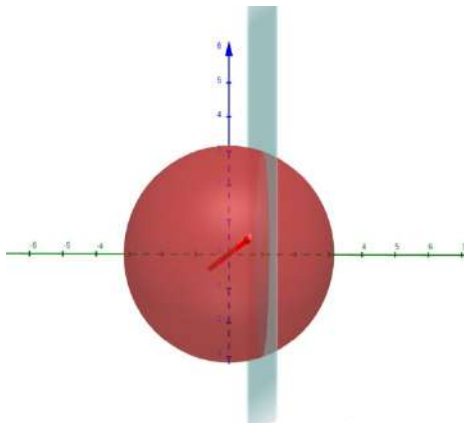
Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), b: t \in \mathbb{R}\}$
 $\{(x, b): x \in \mathbb{R}\};$ where $(a + t) = x$

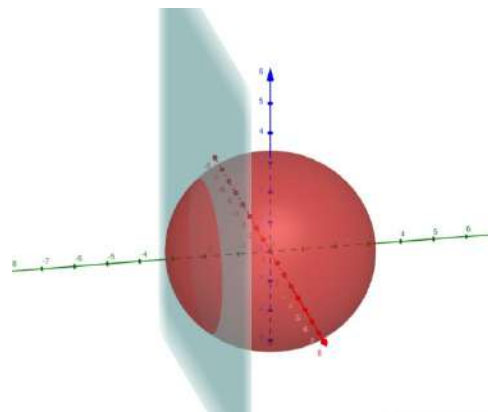
For this case Y coordinate is always b

When $b > 0$, the line is above origin, parallel to X axis

When $b < 0$, the line is below origin, parallel to X axis.



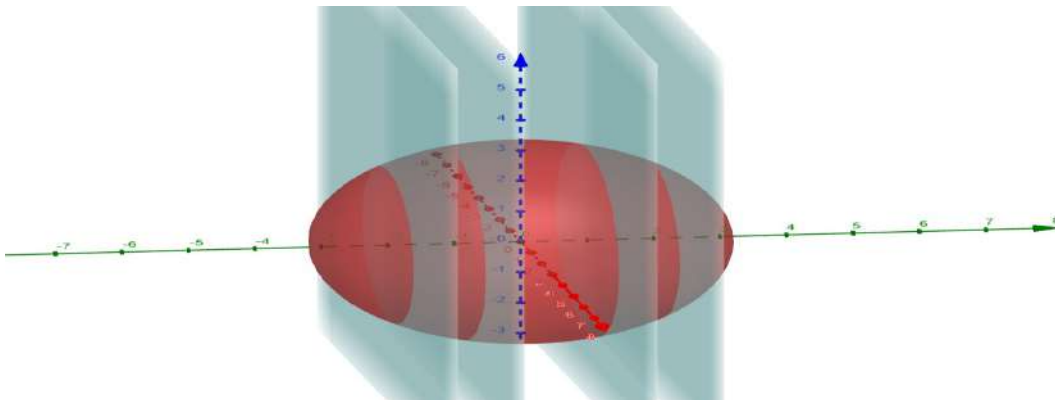
Picture-2



Picture-3

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-4

Blue line= X axis

Green line= Y axis

Red line= Z axis

EXAMPLE-3.2: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map

$$\alpha: G * S \rightarrow S \text{ by } \alpha\{t, (x, y)\} = t. (x, y) := (x, y + t) \forall t \in G \text{ and } (x, y) \in \mathbb{R}^2$$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

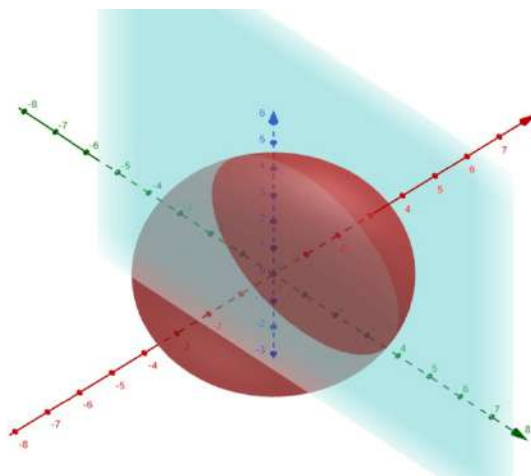
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{1, (1 + t): t \in \mathbb{R}\}$$

$$\{(1, y): x \in \mathbb{R}\}; \text{ where } (1 + t) = y$$

For this case the X coordinate is always 1

i.e. horizontal line parallel to Y axis.



Picture-5

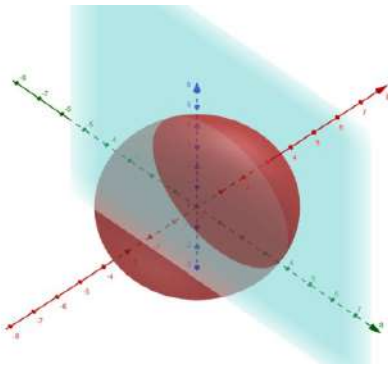
Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{a, (t + b): t \in \mathbb{R}\}$
 $\{(a, y): y \in \mathbb{R}\}$; where $(b + t) = y$

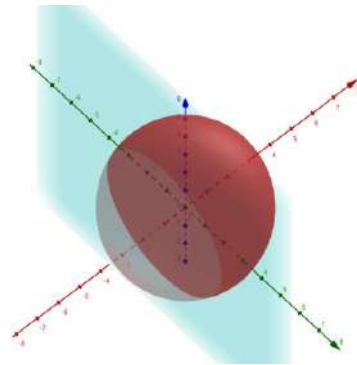
For this case X coordinate is always a

When $a > 0$, the line lies on right side of the origin, parallel to Y axis

When $a < 0$, the line lies on left side of the origin, parallel to Y axis.



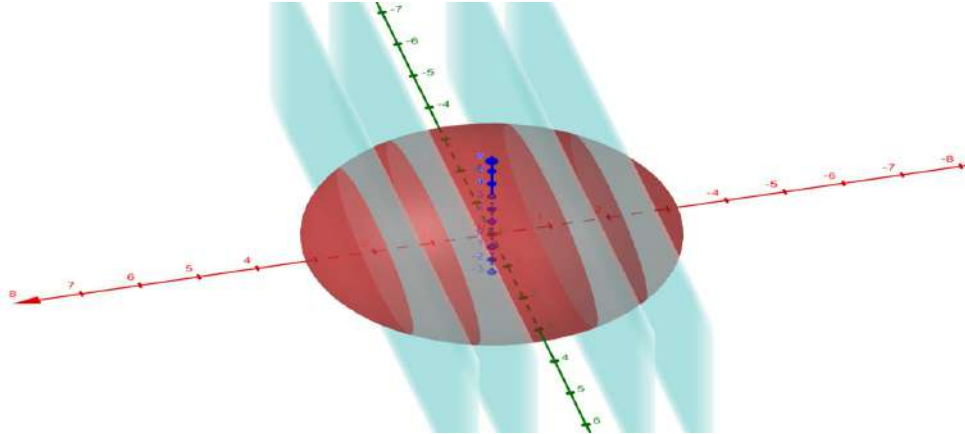
Picture-6



Picture-7

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-8

Blue line= X axis
Green line= Y axis
Red line= Z axis

EXAMPLE-3.3: Let the group $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Let us define a map $\alpha: G * S \rightarrow S$ by $\alpha\{t, (x, y)\} = t. (x, y) := (x + t, y + t) \forall t \in G$ and $(x, y) \in \mathbb{R}^2$

ANSWER: Here the group is $G = (\mathbb{R}, +)$ and the set $S = \mathbb{R}^2$. Clearly S is a G set.

Let us take two points $(1, 1)$ and $(a, b) \in \mathbb{R}^2$

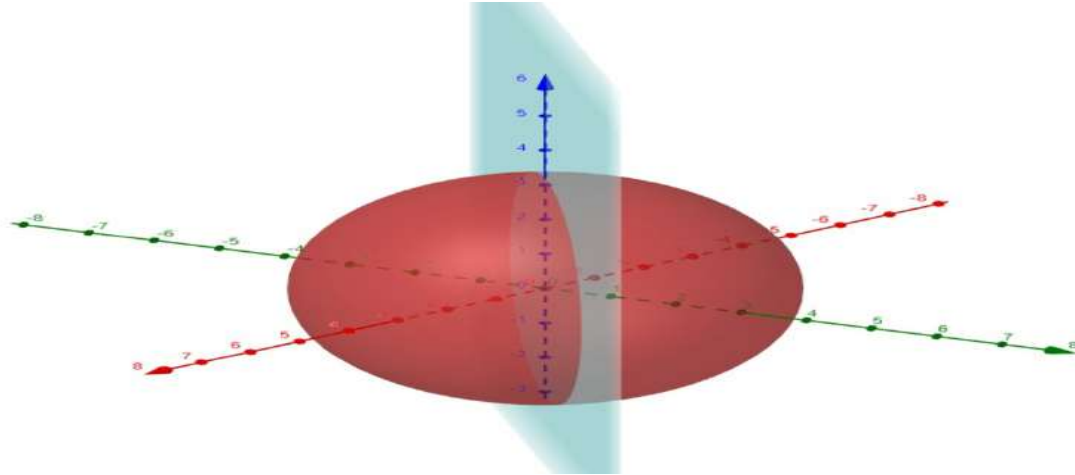
For the point $(1, 1)$, $O_{(1,1)} = \{\varphi(t, (1, 1)): t \in \mathbb{R}\}$

$$\{(1 + t), (1 + t): t \in \mathbb{R}\}$$

$$\{(x, x): x \in \mathbb{R}\} ; \text{ where } (1 + t) = x$$

As x is a arbitrary real number and $y = x$ so it passes through the origin and slope 1.

The picture is given below,



Picture-9

Blue line= X axis
Green line= Y axis
Red line= Z axis

For the point (a, b) $O_{(a,b)} = \{\varphi(t, (a, b)): t \in \mathbb{R}\}$
 $\{(a + t), (t + b): t \in \mathbb{R}\}$

As $t \in \mathbb{R}$ so take two different values of t namely $t = 0$ and $t = 1$

Then we have the required line passes through the points (a, b) & $(a + 1, b + 1)$

Equation of the line will be: $\frac{y - y_2}{y_1 - y_2} = \frac{x - x_2}{x_1 - x_2}$

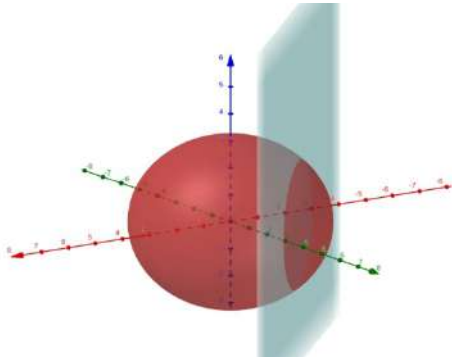
$$\text{Or, } \frac{y - b}{b + 1 - b} = \frac{x - a}{a + 1 - a}$$

$$\text{Or, } x - y = (a - b)$$

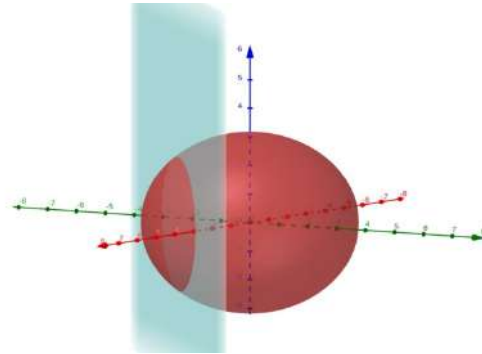
$$\text{Or, } y = x - (a - b)$$

This shows that the slope is 1 but the intercept is non zero.

When $a > b$, the intercept is negative and When $a < b$, the intercept is positive.



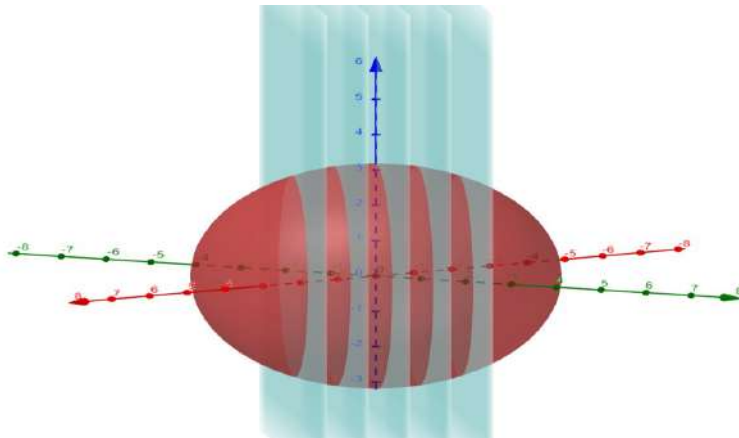
Picture-10



Picture-11

Blue line= X axis
Green line= Y axis
Red line= Z axis

So, the Orbits can be represented by the following picture,



Picture-12

Blue line= X axis
Green line= Y axis
Red line= Z axis

4. Conclusion

Let G be a group and S be a non empty set. Suppose $x \in S$. Then, we wish to find the notation for Orbit of x .

Orbit of x , denoted by

$$\begin{aligned}[x] &= \{g \cdot x : g \in G\} \\ &= \{y \in S : y = g \cdot x \text{ for some } g \in G\} \\ &= \{y \in S : x \sim y\} \\ &= cl(x)\end{aligned}$$

This means Orbits of elements of the non empty set forms a class or precisely forms an equivalence class of x . So it is clear that Orbits follows all properties of an equivalence class. So, our conclusion is,

1. The Orbits of x are either disjoint or equal.
2. The set S is a disjoint union of its Orbits.
3. The Orbits can be uniquely represented geometrically.

5. References

1. Wolfram Math world
2. Fundamentals of Abstract Algebra-
D.S.Malik
John N.Mordeson
M.K.Sen



Department of Mathematics

Akhil Mukherjee Rd, Choudhary Para,
Rahara, West Bengal 700118

PROJECT on

Symmetry Groups of the Platonic Solids

Paper Code - MTMA CC-XII

Submitted by

Name : Subhrangsu Santra

Department : Mathematics

Course : B.Sc

Semester : 5th

College Roll No : 1333

Exam Roll No : 2022151129

Registration No :

A01-1112-113-028-2018

Supervised by

Prof. Pravanjan Kumar Rana
Head of the department

Acknowledgement

With feelings of great pride and respect, we, Rittwik Banerjee & Subhrangsu Santra convey our deep sense of gratitude to our HOD of mathematics, RKMVCC, Mr. Pravanjan Kr. Rana who gave us this wonderful opportunity to work on the project 'Symmetry Groups of Platonic Solids' and also for his sincere guidance and inspiration in completing the project.

Any attempt at any level can't be satisfactorily completed without the support and guidance of parents and friends. We will always be indebted to them.

This study has indeed helped us to explore more knowledgeable avenues related to this topic and I am certain it will help us immensely in future

Content

The Tetrahedron
The Cube and Octahedron
The Dodecahedron and Icosahedron

Symmetry Groups of the Platonic Solids

Intorduction :

From the era of Ancient Greece to the modern day, five important 3-dimensional solids have captured the human imagination, playing an important role across various academic pursuits.

These five polyhedra, the Platonic Solids, have undoubtedly held a fundamental position in mathematical inquiry. From Plato's first postulation of their existence in his dialogue *The Timaeus*, to Euclid's exploration of their properties in his final book of *The Elements*—they've historically been object of mathematical interest. Still, while geometers have studied their mathematical beauty and unique symmetries for millenia , their influence isn't only limited to Mathematics. They've also played an important role in other fields. For example, in early Cosmology, Johannes Kepler used them to explore his first model of the solar system, a step towards geometric classification of planetary movements that lead to his discovery of the properties of elliptic orbits. Additionally, both Biology and Chemistry make use of their properties and symmetries, through the study of virus morphologies and the structures of the interactions of symmetric molecules respectively. Their implications don't end here; the Platonic Solids are undoubtedly important to study.

This paper serves to offer a mathematical overview of the classification of the symmetries of the Platonic Solids, determining the symmetry groups of each polyhedron explicitly.

The Tetrahedron

Proposition 1. Tetrahedra have a rotational symmetry group isomorphic to A_4 and a total symmetry group isomorphic to S_4

First, note that a tetrahedron has four vertices. For each permutation of these vertices, there exists a symmetry in the total symmetry group. Specifically, the first vertex can take four different positions. The second vertex can then end up in any of the three remaining positions via rotation. The third vertex must then take any of the final two positions by reflection, and now the position of the fourth vertex remains fixed. Therefore, under rotations and reflections, the Tetrahedron has $4 * 3 * 2 * 1$ or 24 total symmetries. Observe that the order of S_4 , the Permutation Group of order 4, also has order 24. Now, each vertex can be labeled from 1 to 4, and thus, permutations of vertex positions can be expressed under cyclic notation. Using this notation, first the rotational symmetries can be listed out. A tetrahedron has two axes of symmetry, one passing through the center of one face and the vertex right above it, and another passing through the center of one edge and the perpendicular edge adjacent to it. We can label these axes of symmetry as L and M, respectively.

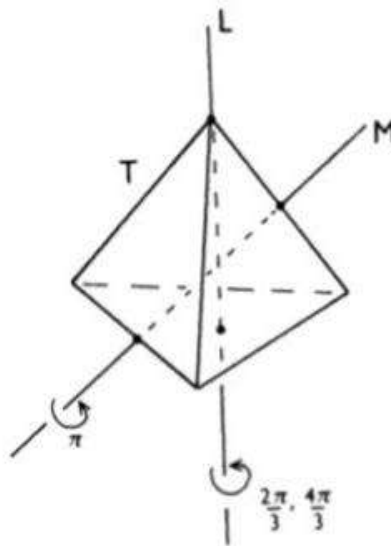


Fig : The axes of symmetry of the Tetrahedron

Clearly, an axis of type L permutes only three vertices, and thus all three cycles of the vertex elements 1, 2, 3, and 4 describe rotations along such axes. Thus, the 8 possible three cycles (123), (132), (124), (142), (134), (143), (234), and (243) correspond to the possible 120 degree symmetry rotation. On the other hand, an axis of type M permutes all four vertices, swapping them in pairs. Thus, the three possible products of two disjoint transpositions, (12)(34), (13)(24), and (14)(23) correspond to elements of the rotational symmetries wherein the solid is revolving 180 degrees. The final rotational symmetry, the identity—not rotating the shape at all—corresponds to the cyclic notation describing no permutations, (). Note that these 12 possible rotational symmetries directly correspond to all even order elements of S_4 , otherwise known as the Alternating Group A_4 . Clearly when two rotations r and r_0 prompt permutations p and p_0 respectively, their composed rotation rr_0 , prompts the permutation pp_0 , exhibiting a homomorphism. Moreover, the injective and surjective mapping explicitly listed out above exhibits a bijection. Thus, via this correspondence, the group of rotational symmetries of the Tetrahedron are isomorphic to A_4 . On a similar note, the possible reflections of the tetrahedron can also be expressed using cyclic Notation. Note that the only possible tetrahedral plane of symmetry would intersect both the midpoint of an edge and the opposite vertices of the two faces containing that edge. Equivalently, a plane of symmetry must be spanned by any two L and M axes of symmetry, and would swap any two vertices of the tetrahedron not contained in this plane. Thus all six transpositions of S_4 , (12), (13), (14), (23), (24), and (34), correspond to a reflectional symmetry. Now, the only Elements that don't correspond to a single reflection or rotation are remaining four cycles (1234), (1243), (1324), (1342), (1423), and (1432). We can see that (1234) is equivalent to the product (123)(34), and moreover, that the corresponding movement matches up with the composition of a reflection and rotation on the solid. Similarly all other elements of S_4 can be mapped to by elements generated by rotations and reflections, and this map is thus surjective. Now, as all 2 elements of S_4 map to the 24 possible rotation and reflection symmetries of the Tetrahedron, and compositions of these elements directly correspond on both sides of the mapping, the full group of symmetries is isomorphic to S_4 .

The Cube and Octahedron

Proposition 2 :Cubes and Octahedra have a rotational symmetry group isomorphic to S_4 and a total symmetry group isomorphic to $S_4 \times Z_2$ under rotational symmetries opposite vertices in a cube can be paired together, as for any rigid rotation of a vertex in a cube, its opposite vertex must move accordingly to remain opposite. Thus, in similar fashion to the argument for the number of total symmetries of a tetrahedron, we can claim that the number of rotational symmetries of a cube is the number ways you can permute these 4 pairs of vertices—if a rotation permuting all vertex couples can be found. Below, we will show that rotations do permute every vertex; it follows that the number of rotational symmetries is 24. There exist three types of axes of symmetry on the cube (Figure 4). The first type, denoted here as L, intersects the midpoint of two faces of the cube. There are three such axes, and each allows three rotational symmetries, by 90, 180, and 270 degree rotations respectively. Thus there exists nine rotations about L axes. Another axis type intersects the midpoint of two opposite edges, denoted here as M. There are six

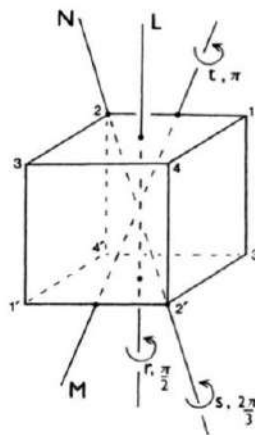


Fig : The axes of symmetry of the cube

such axes, and each has one rotational symmetry of 180 degrees, so there are 6 rotations about M axes. Finally, the last axis type, denoted here as N, intersects two

opposite vertices, and there are 4 opposite vertex pairs as previously stated. On each N axis, there are two allowed symmetries created by rotating the solid by 120 and 240 degrees. Thus, N axes have 8 allowed rotations. In sum, all possible rotations—9, 6, and 8 for each axis type—plus the identity add up to 24 symmetry element.

Using this information, it is possible to show that group of rotations above is isomorphic to S_4 . Numbering the corners on only one face of the cube from 1 to 4 allows us to then number their corresponding opposite vertices from 1' to 4' respectively, differentiating the four permutable constitute of the cube. Now, permutations of these elements directly correspond to permutations in S_4 . Note how rotation about axis types L, M, and N return four cycles, transpositions, and three cycles respectively. Additionally, observe how a product of two rotations clearly induces the correct product of two permutations in S_4 by analysis. A surjective correspondence is bijective if it maps two sets of equal size and the number of rotations found above, 24, is exactly equal to the number of elements in S_4 . Thus the group of rotations of the cube is isomorphic to S_4 . As the rotational symmetry group of the cube is isomorphic to S_4 , the rotational symmetry group of its dual, the octahedron, is also isomorphic to S_4 . Now, the full symmetry groups of a cube and an octahedron must be isomorphic to $S_4 \times \mathbb{Z}_2$

The Dodecahedron and Icosahedron

Proposition 3 : Dodecahedra and icosahedra have a rotational symmetry group isomorphic to A_5 and a total symmetry group isomorphic to $A_5 \times \mathbb{Z}_2$

First, in order to determine the number of rotational symmetries of the dodecahedron, we can count the number of ways we can permute its vertices. Note that the solid has 20 vertices, and each vertex is adjacent to 3 other vertices. Thus, there are 20 places to map our first vertex to. Taking a second vertex that was adjacent to the first vertex, there are only new 3 adjacent spots it can map to. Once two adjacent vertices are fixed, all other vertices under a rigid transformation are

then determined; the number of possible rotations of the dodecahedron is $20 * 3$ or 60. Observe that this is equal to the order of A_5 .

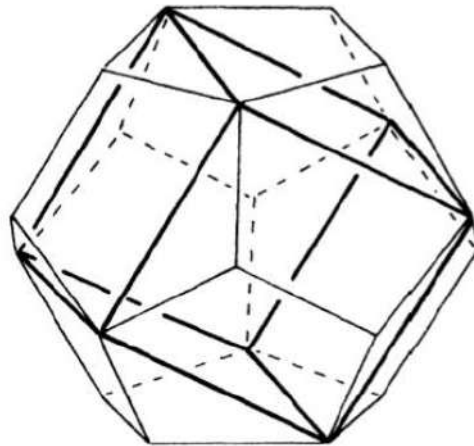


Fig : Inscribed cubes of the dodecahedron.

Similar to the way rotations permute opposite pairs of vertices of the cube as noted above, rotations of the dodecahedron permute five inscribed cubes amongst each other. Observe that the edges of each cube are diagonals of every pentagonal face of the dodecahedron. Moreover, each of the five possible diagonals on every pentagonal face corresponds to one of the five inscribed permutable cubes. We can number each cube by numbering these diagonals on the topmost face of the dodecahedron, starting at the nearest diagonal, and labeling them from 1 to 5 in a clockwise fashion—so that Figure 5 portrays the 5th diagonal and thus cube 5. Now, note that the cube has axes of symmetry that intersect opposite vertices in pairs; there are 10 such axes for the 20 vertices. Moreover, as each vertex connects three edges, and they must map to each other in a rotational symmetry about that vertex, these axes have only 2 rotational symmetry elements of 120 and 240 degrees. Therefore there are 20 total rotational symmetries among these axes, and we can show they correspond to the 20 3-cycles in A_5 . Choosing one such axes of symmetry, we can see that its rotations fix the two inscribed cubes whose N axes (as labeled in the last section, Figure 4) intersect the same two vertices. Note that the N axis has rotational symmetries of 120 and 240 degrees, equivalent to the

rotations exhibited by the dodecahedron we investigate. Now, there are three remaining inscribed cubes not-fixed by rotations by each axes of symmetry and thus must be sent to each other. These cubes can be represented by their numbered face diagonal per the labeling scheme above. Thus each rotation among these axes directly corresponds to a permutation of three cubes, or a 3-cycle in S_5 . In fact, as there exist 20 unique rotational symmetries along the 10 diagonals, 20 unique 3-cycles can be expressed. There are a total of 20 unique 3-cycles possible in S_5 , so these rotational elements must correspond to all 3-cycles in S_5 .

Finally, for $n \geq 3$ the 3-cycles generate A_n , so all the 3-cycle permutations mapped to in S_5 generate A_5 . This is clearly a homomorphism, as combination of rotations clearly correspond to associated permutation groups in A_5 by definition. Moreover, the map criteria described above details a bijection; it is surjective as all elements in A_5 could be mapped to by Theorem 6.5, and both sets have order 60 as shown at the start of this section. Thus there exists an isomorphism between A_5 and the rotational symmetry group of the dodecahedron. As the rotational symmetry group of the dodecahedron is isomorphic to A_5 , the rotational symmetry group of its dual, the icosahedron, is also isomorphic to A_5 . Now the Full Symmetry Groups of a dodecahedron and a icosahedron must be isomorphic to $A_5 \times Z_2$.

Concluding Remarks

Tetrahedra were found to have a rotational symmetry group isomorphic to S_4 . Cubes & octahedra have a rotational symmetry group isomorphic to S_4 and a total symmetry group isomorphic to $S_4 \times Z_2$. Finally dodecahedra and icosahedra have a rotational symmetry group isomorphic to A_5 and a total symmetry group isomorphic to $A_5 \times Z_2$, completing the classification of these symmetries.

References

1. M. A. Armstrong, Groups and Symmetry, Springer, New York, 1988
2. O'Connor, John, Symmetry Groups of Platonic Solids, 2003
3. Groups and Symmetry, a guide to discovering mathematics, David W. Farmer
4. Wikipedia
5. YouTube



2021-2022

TOPIC-EXTERNAL DIRECT PRODUCT AND ITS
APPLICATION

NAME-SUMIT PARAMANIK

EXAM ROLL NO.-2022151109

REGISTRATION NO.-A01-1152-113-022-2019

PAPER- CC-XII

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my advisor Prof. Peavanjan Kumar Rana , who introduced me to the wonderful project work . I would also like to thank him for the guidance , patience and help and for contributing from his abundance experience , knowledge and wisdom . It was an honour for me to get a glimpse to his world and way of thinking .My friend Agniva Banerjee and Akram Khan also helped me to do the project work , I am also thankful them.

External Direct Product and its application

Abstract:-

External direct product is one of the most important part of group theory .We are going to introduce an idea how the external direct product help us in data science , public Key Cryptography,digital signature ,genetics and electrical circuits .

Introduction:-

In this project, we show how to piece together groups to make large groups. Previously, we will show that we can often start with one large group and decompose it into a product of smaller groups in much the same way as a composite positive integer can be broken down into a product of primes. These methods will later be used to give us a simple way to construct all finite abelian groups.

Definition :

Let G_1, G_2, \dots, G_n be a finite collection of groups. The external direct product of G_1, G_2, \dots, G_n , written as $G_1 \times G_2 \times \dots \times G_n$, is the set of all n -tuples for which the i th component is an element of G_i and **the operation is component wise**.

The resulting algebraic object satisfies the axioms for a group. Specifically:

Associativity :-

The binary operation on $G \times H$ is associativity.

Identity :-

The direct product has an identity element, namely $(1_G, 1_H)$, where 1_G is the identity element of G and 1_H is the identity element of H .

Inverses :-

The inverses of an element (g, h) of $G \times H$ is the pair (g^{-1}, h^{-1}) , where g^{-1} is the inverse of g in G , and h^{-1} is the inverse of h in H .

Hence, external direct product form a group.

In symbols, $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i\}$, Where $(g_1, g_2, \dots, g_n)(g_1', g_2', \dots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \dots, g_n g_n')$. It is understood that each product $g_i g_i'$ is performed with the operation of G_i . We leave it to the reader to show that the external direct product of groups is itself a group.

Properties of external direct product:-

1. Order of $(G_1 \times G_2 \times G_3 \times \dots \times G_k) = |G_1| \cdot |G_2| \cdot |G_3| \cdot \dots \cdot |G_k|$

2. The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols, $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$.

Proof : Denote the identity of G_i by e_i . Let $s = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$ and $t = |(g_1, g_2, \dots, g_n)|$. Because s is a multiple of each $|g_i|$ implies that $(g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (e_1, e_2, \dots, e_n)$, we know that $t \leq s$. On the other hand, from $(g_1, g_2, \dots, g_n)^t = (g_1^t, g_2^t, \dots, g_n^t) = (e_1, e_2, \dots, e_n)$ we see that t is a common multiple of $|g_1|, |g_2|, \dots, |g_n|$. Thus, $s \leq t$. If $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$ is an external direct product, say $(g_1, g_2, g_3, \dots, g_k) \in \text{EDP}$ Now, $(g_1, g_2, g_3, \dots, g_k)$ is just an element of $(G_1 \times G_2 \times G_3 \times \dots \times G_k)$

Application :-

We conclude this project with five applications of the material presented here—three to cryptography, the science of sending and deciphering secret messages, one to genetics, and one to electric circuits.

Application to Data Security :-

Because computers are built from two-state electronic components, it is natural to represent information as strings of 0s and 1s called binary strings. A binary string of length n can naturally be thought of as an element of $Z_2 \times Z_2 \times \dots \times Z_2$ (n copies) where the parentheses and the commas have been deleted. Thus the binary string 11000110 corresponds to the element $(1, 1, 0, 0, 0, 1, 1, 0)$ in $Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_2$. Similarly, two binary strings $a_1 a_2, \dots, a_n$ and b_1, b_2, \dots, b_n are added component wise modulo 2 just as their corresponding elements in $Z_2 \times Z_2 \times \dots \times Z_2$ are. For example,

$$11000111 + 01110110 = 10110001$$

And,

$$10011100 + 10011100 = 00000000.$$

The fact that the sum of two binary sequences $a_1a_2 \dots a_n = b_1b_2 \dots b_n = 00 \dots 0$ if and only if the sequences are identical is the basis for a data security system used to protect internet transactions.

Suppose that you want to purchase a compact disc from **www.Amazon.com**. Need you be concerned that a hacker will intercept your credit-card number during the transaction? As you might expect, your credit-card number is sent to Amazon in a way that protects the data. We explain one way to send credit-card numbers over the Web securely. When you place an order with Amazon the company sends your computer a randomly generated string of 0's and 1's called a key. This key has the same length as the binary string corresponding to your credit-card number and the two strings are added (think of this process as "locking" the data). The resulting sum is then transmitted to Amazon. Amazon in turn adds the same key to the received string which then produces the original string corresponding to your credit card number (adding the key a second time "unlocks" the data).

To illustrate the idea, say you want to send an eight-digit binary string such as $s = 10101100$ to Amazon (actual credit-card numbers have very long strings) and Amazon sends your computer the key $k = 00111101$. Your computer returns the string $s + k = 10101100 + 00111101 = 10010001$ to Amazon, and Amazon adds k to this string to get $10010001 + 00111101 = 10101100$, which is the string representing your credit-card number. If someone intercepts the number $s + k = 10010001$ during transmission it is no value without knowing k . The method is secure because the key sent by Amazon is randomly generated and used only one time. You can tell when you are using an encryption scheme on a web transaction by looking to see if the web address begins with "https" rather than the customary "http." You will also see a small padlock in the status bar at the bottom of the browser window.

Application to Public Key Cryptography :-

In the mid-1970s, Ronald Rivest, Adi Shamir, and Leonard Adleman devised an ingenious method that permits each person who is to receive a secret message to tell publicly how to scramble messages sent to him or her. And even though the method used to scramble the message is known publicly, only the person for whom it is intended will be able to unscramble the message. The idea is based on the fact that there exist efficient methods for finding very large prime numbers (say about 100 digits long) and for multiplying large numbers, but no one knows an efficient algorithm for factoring large integers (say about 200 digits long). So, the person who is to receive the message chooses a pair of large primes p and q and chooses an integer r with $1 < r < m$, where $m = \text{lcm}(p - 1, q - 1)$, such that r is relatively prime to m (any such r will do). This person calculates $n = pq$ and announces that a message M is to be sent to him or her publicly as $M_r \bmod n$. Although r , n , and M_r are available to everyone, only the person who knows how to factor n as pq will be able to decipher the message. To present a simple example that nevertheless illustrates the principal features of the method, say we wish to send the message "YES." We convert the message into a string of digits by replacing A by 01, B by 02, . . . , Z by 26, and a blank by 00. So, the message YES becomes 250519. To keep the numbers involved from becoming too unwieldy, we send the message in blocks of four digits and fill in with blanks when needed. Thus, the message YES is represented by the two blocks 2505 and 1900. The person to whom the message is to be sent has picked two primes p and q , say $p = 37$ and $q = 73$ (in actual practice, p and q would have 100 or so digits), and a number r that has no prime divisors in common with $\text{lcm}(p - 1, q - 1) = 72$, say $r = 5$, and has published $n = 37 * 73 = 2701$ and $r = 5$ in a public directory. We will send the "scrambled" numbers $(2505)_5 \bmod 2701$ and $(1900)_5 \bmod 2701$ rather than 2505 and 1900, and the receiver will unscramble them. We show the work involved for us and the receiver only for the block 2505. The arithmetic involved in computing these numbers is simplified as follows:

$$2505 \bmod 2701 = 2505$$

$$(2505)^2 \bmod 2701 = 602$$

$$(2505)^4 \bmod 2701 = (602)(602) \bmod 2701 = 47$$

$$\text{So, } (2505)^5 \bmod 2701 = (2505)(47) \bmod 2701 = 2415.$$

Thus, the number 2415 is sent to the receiver. Now the receiver must take this number and convert it back to 2505. To do so, the receiver takes the two factors of 2701, $p = 37$ and $q = 73$, and calculates the least common multiple of $p - 1 = 36$ and $q - 1 = 72$, which is 72 (This is where the knowledge of p and q is necessary.) Next, the receiver must find $s = r^{-1}$ in $U(72)$ —that is, solve the equation $5 * s = 1 \bmod 72$. This number is 29. (There is a simple algorithm for finding this number.) Then the receiver takes the number received, 2415, and calculates $(2415)^{29} \bmod 2701$. This calculation can be simplified as follows:

$$2415 \bmod 2701 = 2415$$

$$(2415)^2 \bmod 2701 = 766$$

$$(2415)^4 \bmod 2701 = (766)^2 \bmod 2701 = 639$$

$$(2415)^8 \bmod 2701 = (639)^2 \bmod 2701 = 470$$

$$(2415)^{16} \bmod 2701 = (470)^2 \bmod 2701 = 2119$$

$$\text{So, } (2415)^{29} \bmod 2701 = (2415)^{16} (2415)^8 (2415)^4 \bmod 2701 =$$

$$(2119)(470)(639)(2415) \bmod 2701 = ((2119)(470) \bmod 2701 * (639)(2415) \bmod 2701) \bmod 2701$$

5(1962)(914) mod 2701 52505. [We compute the product (2119)(470)(639)(2415) in two stages so that we may use a hand calculator.]

Thus the receiver correctly determines the code for "YE." On the other hand, without knowing how pq factors, one cannot find the modulus (in our case, 72) that is needed to determine the intended message.

Application to Digital Signatures :-

With so many financial transactions now taking place electronically, the problem of authenticity is paramount. How is a stockbroker to know that an electronic message she receives that tells her to sell one stock and buy another actually came from her client? The technique used in public key cryptography allows for digital signatures as well. Let us say that person A wants to send a secret message to person B in such a way that only B can decode the message and B will know that only A could have sent it. Abstractly, let E_A and D_A denote the algorithms that A uses for encryption and decryption, respectively, and let E_B and D_B denote the algorithms that B uses for encryption and decryption, respectively. Here we assume that E_A and E_B are available to the public, whereas D_A is known only to A and D_B is known only to B and that $D_B E_B$ and $E_A D_A$ applied to any message leaves the message unchanged. Then A sends a message M to B as $E_B(D_A(M))$ and B decodes the received message by applying the function $E_A D_B$ to it to obtain

$$(E_A D_B)(E_B(D_A(M))) = E_A(D_B E_B)(D_A(M)) = E_A(D_A(M)) = M.$$

Notice that only A can execute the first step [i.e., create $D_A(M)$] and only B can implement the last step (i.e., apply $E_A D_B$ to the received message).

Transactions using digital signatures became legally binding in the United States in October 2000.

Application to Genetics :-

The genetic code can be conveniently modeled using elements of $Z_4 \times Z_4 \times \dots \times Z_4$ where we omit the parentheses and the commas and just use strings of 0s, 1s, 2s, and 3s and add component wise modulo 4. A DNA molecule is composed of two long strands in the form of a double helix. Each strand is made up of strings of the four nitrogen bases adenine (A), thymine (T), guanine (G), and cytosine (C). Each base on one strand binds to a complementary base on the other strand. Adenine always is bound to thymine, and guanine always is bound to cytosine. To model this process, we identify A with 0, T with 2, G with 1, and C with 3. Thus, the DNA segment ACGTAACAGGA and its complement segment TGCATTGTCCT are denoted by

03120030110 and 21302212332. Noting that in Z_4 , $0 + 2 = 2$, $2 + 2 = 0$, $1 + 2 = 3$, and $3 + 2 = 1$, we see that adding 2 to elements of Z_4 interchanges 0 and 2 and 1 and 3. So, for any DNA segment $a_1 a_2 \dots a_n$ represented by element of $Z_4 \times Z_4 \times \dots \times Z_4$, we see that its complementary segment is represented by $a_1 a_2 \dots a_n + 22 \dots 2$.

Application to Electric Circuits :-

Many homes have light fixtures that are operated by a pair of switches. They are wired so that when either switch is thrown the light changes its status (from on to off or vice versa). Suppose the wiring is done so that the light is on when both switches are in the up position. We can conveniently think of the states of the two switches as being matched with the elements of $Z_2 \times Z_2$ with the two switches in the up position corresponding to (0, 0) and the two switches in the down position corresponding to (1, 1). Each time a switch is thrown, we add 1 to the corresponding component in the group $Z_2 \times Z_2$. We then see that the lights are on when the switches correspond to the elements of the subgroup $\{(1, 1)\}$ and are off when the switches correspond to the elements in the coset $(1, 0) + (1, 1)$. A similar analysis applies in the case of three switches with the subgroup $\{(0, 0, 0), (1, 1, 0), (0, 1, 1), (1, 0, 1)\}$ corresponding to the lights-on situation

Conclusion:-

The role of external direct product in modern algebra cannot describe in a sentence. The use of external direct product is not only limited in group theory but also we can see the use of it in many branches of mathematics like topology and so on. If we come out from algebra then we can see that external direct product also plays a vital role in our daily life. So we can say a mathematics student should know the application of mathematics in daily life

References:-

1. John B. Fraleigh ,A first course of Abstract Algebra ,7th Ed.,pearson 2007
2. Joseph A. Gallian , Contemporary Abstract Algebra,4th Ed. Narosa Publishing House,1999
3. D.S.Malik, John M. Mordeson and M.K.Sen, Fundamental of Abstract Algebra

PROJECT
on
“Group Theory”

Topic : - “Geometrical Interpretation of group Theory on Rubik's Cube”

Paper Code: MTMA CC-XII

Submitted by

Name : Supriya Pan

Department : Mathematics

Course : B.SC

Semester : 5th

College Roll No : 1305

Exam Roll No : 2022151128

**Registration No : A01-1112-113-005-2018 of
2018-2019**

Supervised by

Prof. Pravanjan Kumar Rana

Head of the Department



Department Of Mathematics ,

Ramakrishna Misson Vivekananda Centenary College

Akhil Mukherjee Rd, Chowdhary Para,Rahara,

Khardaha, West Bengal 700118

Acknowledgment

As the students of mathematics of RKMVCC , I, **Supriya Pan** are very grateful to our HOD of Mathematics department, **Prof. Pravanjan Kumar Rana** to encourage us to do this project based on the application of group theory in real world. He taught us the signification of group theory through that's what I decided to do. I learnt a lot of things from this project work. My topic is "**Geometrical Interpretation of Group Theory on Rubik's Cube**", which help us in doing a lot of Research and we came to know so many things. Since this is a group project work, I would like to thank the rest of my team members **Arijit Majumder , Satyajit Roy** for helping me to complete this project work.

I would also like to thank our college for providing me all necessary resources for this project. All in all, I would like to thank everyone involved in this project and to help me with their suggestions to make the project better.

Contents

Abstract	3
1 Introduction	3
2 Rubik's Cube	4
3 Singmaster Notation	4
4 Permutation Group	5
4.1 Defination	5
5 Dihedral Group	6
6 Wreath Product	7
6.1 Defination	7
7 The Rubik's Cube Group	7
7.1 Edge Cubes	8
7.2 Corner Cubes	8
7.3 Cube Position	9
7.3.1 Example	9
7.3.2 Example	9
7.3.3 Remark	10
7.4 The Illegal Rubik's Cube Group	10
8 Fundamental Theorems of Cube Theory	10
8.1 First Fundamental Theorem of Cube Theory	11
8.2 Second Fundamental Theorem of Cube Theory	11
9 Application of the Legal Rubik's Cube Group	11
10 Sylow Theorems	12
10.1 The First Sylow Theorem	12
10.2 The Second Sylow Theorem	12
10.3 The Third Sylow Theorem	12
11 Application of Sylow Theorems on Rubik's Cube	12
12 Concluding Remarks	13
13 Reference	13

Geometrical Interpretation of Group Theory on Rubik's Cube

Supriyo Pan(1305),Arijit Majumder(1367),Satyajit Roy(320)

Abstract

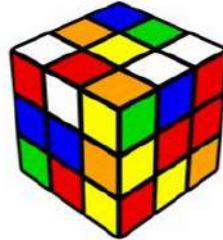
A group is a mathematical object of great importance, but the usual study of group theory is highly abstract and therefore difficult for many people to understand. A very important class of groups are so-called permutation groups which are very closely related to Rubik's cube. Thus, in addition to being a fiendishly difficult puzzle, Rubik's cube provides many concrete examples of groups and of applications of group theory. In this document, we'll alternate between a study of group theory and of Rubik's cube, using group theory to find tools to solve the cube and using the cube to illustrate many of the important topics in group theory.

1 Introduction

Invented in 1974 by Ernő Rubik, a professor of architecture living in Budapest, Hungary. now a days, the Rubik's Cube is one of the popular toys in the world. First, some quick notation. The word "cube" will usually refer to the entire cube that appears to be divided into 27 smaller cubes. We shall call these smaller cubes "cubies", of which 26 are visible. There are three types of cubies: some show only one face called "face cubies" or "center cubies", some show two faces, called "edge cubies" and some show three: the "corner cubies". The entire cube has six faces, each of which is divided into 9 smaller faces of the individual cubies. When it is important to distinguish between the faces of the large cube and the little faces on the cubies, we'll call the little faces "facelets". A permutation is a rearrangement of things. If you consider the "things" to be the facelets on Rubik's cube, it is clear that every twist of a face is a rearrangement of those facelets. Obviously, in Rubik's cube there are constraints on what rearrangements are possible, but that is part of what makes it so interesting. The three facelets that appear on a particular corner cubie, for example, will remain next to each other in every possible rearrangement. A good understanding of permutations and how they behave will help you to learn to effectively manipulate and solve Rubik's cube. The cube, however, has 54 visible facelets, so each cube movement effectively rearranges many of the 54 items. The best way to learn about any mathematical subject is to begin by looking at smaller, simpler cases. Thus in the first part of this document we'll look at permutations of small numbers of items, where we can list all the possibilities and easily keep everything in mind. When we talk about general properties of permutations in the following text, try to think about what these statements mean in the context of a few concrete examples. Rubik's cube is one such concrete example, and we'll introduce a few others as we proceed.

2 Rubik's Cube

The Rubik's Cube is a $3 \times 3 \times 3$ cube. The cube can be manipulated by rotating the faces of the cube. There are six faces, with each face composed of nine facets. On each face, the center facet is fixed, and is unmoveable. In total, there are $6 \cdot 9 = 54$ facets on the cube. Each facet is also coloured, and solving the cube requires that each face be a solid colour. That is, the nine facets of the side must all be the same colour. As well as some of the associated theorems and applications of the group. Below is a picture of what a cube looks like :

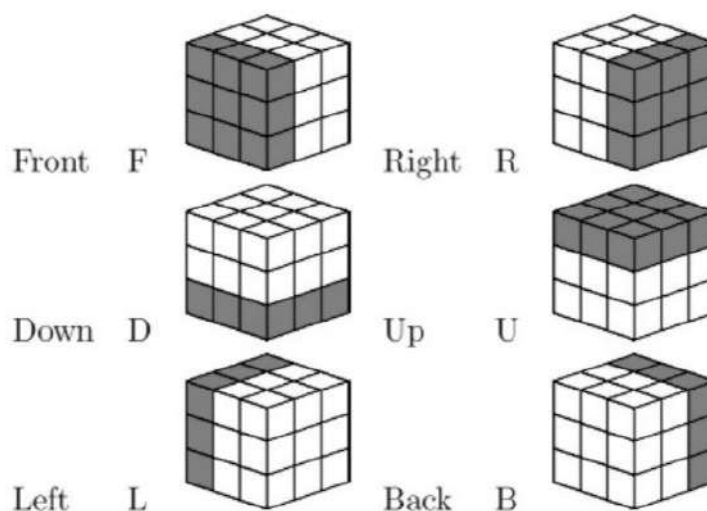


A General Puzzled Rubik's Cube

3 Singmaster Notation

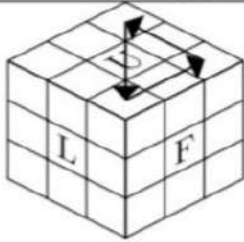
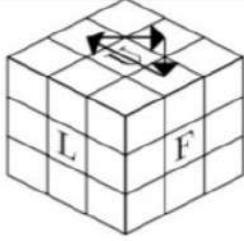
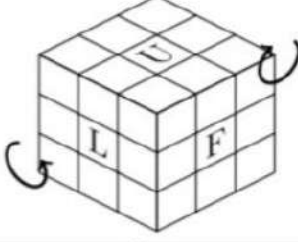
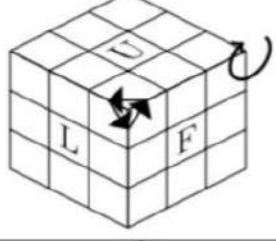
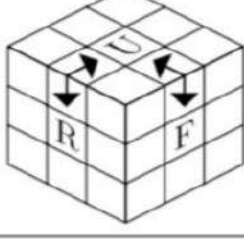
The notations are introduced by David Singmaster

- Let U denote the upward (top) face.
- Let F denote the front face.
- Let L denote the left face.
- Let R denote the right face.
- Let B denote the back face.
- Let D denote the downward (bottom) face.



The inverse of each move would be the 90 degree rotation of the face counter-clockwise and denoted by M_i^{-1} ,

where $M_i \in \{F, L, U, R, B, D\} \rightarrow$ The inverse of the combination FLU is $(FLU)^{-1}$ i.e. $U^{-1}L^{-1}F^{-1}$.

Move Sequence [1]	Diagram [6]
$RB^{-1}RF^2R^{-1}BRF^2R^2$	
$R^2UFB^{-1}R^2F^{-1}BUR^2$	
$(R^{-1}D^2RB^{-1}U^2B)^2$	
$R(U^2RF^{-1}D^2FR^{-1})^2R^{-1}$	
$LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$	

4 Permutation Group

4.1 Defination

A bijective function $\phi : A \rightarrow A$ is called permutation on A.the set

$$\mathcal{G}_A = \{ \phi | \phi : A \rightarrow A \text{ is a bijective function} \}$$

consisting of all permutations on A is a group with respect to the composition of functions and it is called the Permutation group on A.

To see that \mathcal{G}_A is indeed a group with respect to the composition of functions, observe that

1. If $\phi, \psi \in \mathcal{G}_A$, then obviously the composition function $\phi\psi \in \mathcal{G}_A$.
2. Since the composition is associative, thus for any $\phi, \psi, \chi \in \mathcal{G}_A$.
3. The function $I : A \rightarrow A$ defined as $I(a) = a, \forall a \in A$

$$I\phi = I = \phi I$$

Thus I is identity.

4. For each $\phi \in \mathcal{G}_A, \exists$ a bijective function $\phi^{-1} : A \rightarrow A$ such that

$$\phi^{-1}\phi = I = \phi\phi^{-1}$$

Clearly, $\phi^{-1} \in \mathcal{G}_A$ and it is the inverse of ϕ .

Thus all the four conditions of a group is satisfied, hence is a group with respect to the composition of functions.

Thus given any non-empty set A , there exists a permutation group given by

$$\mathcal{G}_A = \{ \phi \mid \phi : A \rightarrow A \text{ is a bijective function} \}$$

But from now onwards we will consider only non-empty finite sets and hence will be dealing with permutation group on a finite set. Further for any finite set A of cardinality n , a one-to-one correspondence exists between the elements of A and the set $\{1, 2, 3, \dots, n\}$. Thus to study permutation group of finite sets it is enough to study the permutation groups of the sets $\{1, 2, 3, \dots, n\}$ for any positive integer n .

we denoted by S_n , the permutation group on $\{1, 2, 3, \dots, n\}$ i.e.,

$$S_n = \{ \phi \mid \phi : \{1, 2, 3, \dots, n\} \rightarrow \{1, 2, 3, \dots, n\} \}$$

The permutation group S_n is also known as the symmetric group of degree n .

5 Dihedral Group

The Dihedral group D_n is the group of symmetries of a regular polygon with n vertices. We think of this polygon as having vertices on the unit circle, with vertices labeled $0, 1, 2, \dots, n-1$ starting at $(1, 0)$ and

proceeding counterclockwise at angles in multiples of $360/n$ degrees, that is, $2\pi/n$ radians.

There are two types of symmetries of the n -gon, each one giving rise to n elements in the group D_n :

- Rotations $R_0, R_1, R_2, \dots, R_{n-1}$ where R_k is rotation of angle $2\pi k/n$.
- Reflections $S_0, S_1, S_2, \dots, S_{n-1}$, where S_k is reflection about the line through the origin and making an angle of $k\pi/n$ with the horizontal axis.

The group operation is given by composition of symmetries: if a and b are two elements in D_n , then $a \cdot b = b \circ a$. That is to say, $a \cdot b$ is the symmetry obtained by applying first a , followed by b . The elements of D_n can be thought as linear transformations of the plane, leaving the given n -gon invariant. This lets us represent the elements of D_n as 2×2 matrices, with group operation corresponding to matrix multiplication. Specifically,

$$R_k = \begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix},$$

$$S_k = \begin{pmatrix} \cos(2\pi k/n) & \sin(2\pi k/n) \\ \sin(2\pi k/n) & -\cos(2\pi k/n) \end{pmatrix}.$$

It is now a simple matter to verify that the following relations hold in D_n :

$$\begin{aligned} R_i \cdot R_j &= R_{i+j} \\ R_i \cdot S_j &= S_{i+j} \\ S_i \cdot R_j &= S_{i-j} \\ S_i \cdot S_j &= R_{i-j} \end{aligned}$$

where $0 \leq i, j \leq n-1$ and both $i+j$ and $i-j$ are computed modulo n . The Cayley table for D_n can be readily computed from the above relations. In particular, we see that R_0 is the identity, $R_i^{-1} = R_{n-i}$ and $S_i^{-1} = S_i$.

6 Wreath Product

The product of two groups can be generalized from semi-direct products even further to wreath products. So below, we discussed the definition of Wreath product,

6.1 Definition

Let, X be a finite set, G be a group and H a group acting on X . Fix a labelling of X , say $\{x_1, x_2, x_3, \dots, x_t\}$ with $|X|=t$. Let, G^t be the direct product of G with itself ' t ' times. Then the wreath product of G and H is $G^t \wr H = G^t \rtimes H$, where H acts on G^t by its action on X .

7 The Rubik's Cube Group

On the Rubik's Cube, there are 54 facets that can be arranged and rearranged through twisting and turning the faces. Any position of the cube can be described as a permutation from the solved state. Thus, the Rubik's Cube group is a subgroup of a permutation group of 54 elements.

The permutation group $G = \langle F, L, U, D, R, B \rangle \subset S_{54}$ is called the Rubik's Cube Group.

There are two different classifications of the Rubik's Cube Group that is the Legal Rubik's Cube Group and the Illegal Rubik's Cube Group. The difference between the two being that the Illegal Rubik's Cube Group allows the solver to take the cube apart and rearrange the facets. In neither case is the solver allowed to remove the stickers from each facet. As expected, the Rubik's Cube Group is a subset of the Illegal Rubik's Cube group.

Now, not all of the permutations of S_{54} will be possible on the Rubik's Cube. The middle facet on each side of the cube is fixed and cannot be permuted to a different position on the cube. Furthermore, any valid permutation on the cube will send corner facets to corner positions and edge facets to edge positions. Any other permutations will not be physically possible on the cube. Hence, G is only a subset of S_{54} and not isomorphic to the full permutation group.

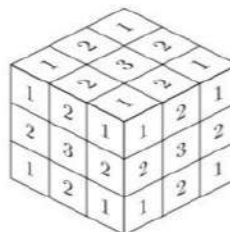


Figure 1. The different types of facets on a Rubik's Cube: 1 denotes the facets that make up corner cubes, 2 denotes facets that make up edge cubes and 3 denotes the fixed center cubes

7.1 Edge Cubes

Every edge cube in the Rubik's Cube consists of two facets, as shown in 1 and there are 12 edge cube on the Rubik's Cube. Note that for every edge cube, each of the two facets of an edge cube lie on different faces of the cube.

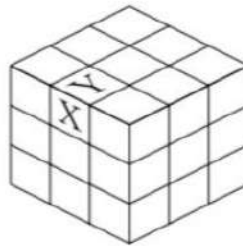


Figure 2. The 2 facets that make up an edge cube [6]

As in figure 2, facet X is on the left face and facet Y is on the upper face. Likewise, it is also possible for facets X and Y to switch places. That is, facet X would be repositioned to where facet Y is and facet Y would be moved to the position where facet X is. In terms of groups, the facets of any edge cube belong to the cyclic group of two elements C_2 . In addition, there are 12 edge cubes on the Rubik's Cube and any edge cube can occupy an edge cube spot. Thus any facet of an edge cube will be in the set $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 = 12_{C_2}$

Likewise to describe the different arrangements of the edge cubes. There are 12 edge cubes on the Rubik's Cube and any edge cube can be in an edge cube spot. Thus, the possible arrangements of the edge cubes of the Rubik's Cube can be described by the permutation group of 12 elements, S_{12} .

(i). The position of all of the edge facets on the Rubik's Cube can be described by the group $12_{C_2} \wr S_{12}$

7.2 Corner Cubes

As shown in Figure 1, each corner cube consists of three facets. Now, there are a total of eight corner cubes on a Rubik's Cube and each of the facets that comprise the corner cube lie on three different sides of the cube.

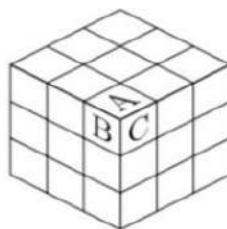


Figure 3. The 3 facets that make up a corner cube

As shown in Figure 3, facet A is on the upper face, facet B is on the left face, and facet C is on the front face. Now, it is possible to reorient the facets of a corner cube: facet A is in the position where facet B is, facet B is moved to where facet C was, facet C moved to the position of facet B; and facet A can be moved to the position of facet C, facet C to the position of facet B and facet B to the position of facet A. In terms of groups, this means that the facets of a corner cube belong

to the cyclic group of three elements C_3 . Moreover, since there are eight corner cubes, the orientation of any facet of a corner cube can be described by the set $C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 = 8_{C_3}$

7.3 Cube Position

Any corner cube be expressed as a 8-tuple and we know any edge cube position can be expressed as a 12-tuple. However, to determine the individual components of the tuples, a fixed numbering system will be needed.

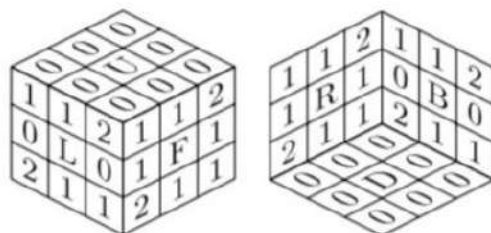


Figure 4. The fixed orientation markings, as denoted for the facets of the Rubik's Cube

For any arbitrary facet, the position of the facet is assigned the corresponding number above. Even though the facets will be moving around the cube, the numbering system remains fixed.

7.3.1 Example

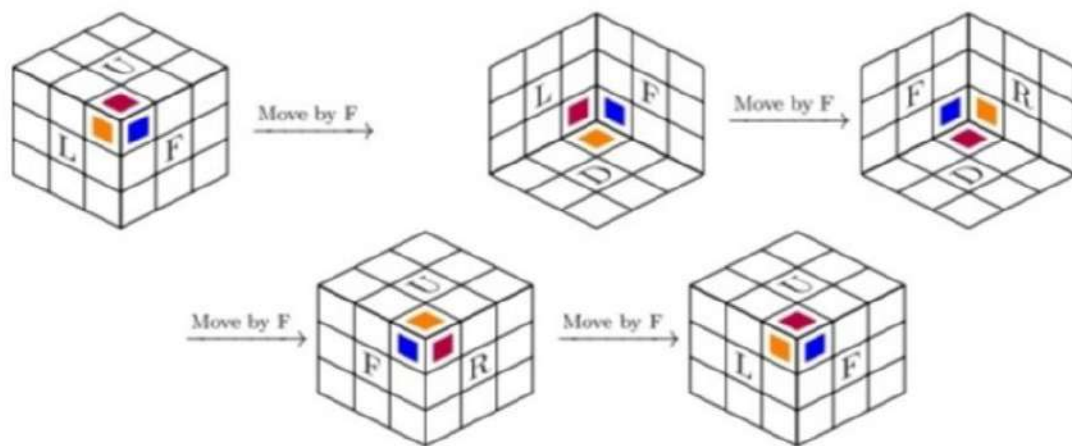
Consider the top edge cube on the front face of the Rubik's Cube [6]. It begins with a number of 1. Now, by doing the move FR, the facet is moved to the upper face on the right side. This position of the edge cube is assigned the number 0.



Figure 5. With each turn, the edge cube's orientation number is changed by either $0 \bmod 2$ or $1 \bmod 2$.

7.3.2 Example

Consider the cube below [6] and the upper, front and left face corner cube.



Tracking the blue facet, it begins with the number 1, then has number 2, number 1, number 2, and then back to number 1 to complete the cycle. Next, the purple facet starts with number 0, then goes to number 1, number 0, number 1, and then back to 0 to complete the cycle. Finally, the orange facet starts with number 2, then number 0, number 2, number 0, and then back to number 2

7.3.3 Remark

With each turn of the R; L; F or B face, the corner facet orientation number is changed by either 1 mod 3 or 2 mod 3. With each turn of the U or D face, the numbering remains unchanged (0 mod 3).

The orientation number for any facet is determined by comparing the position of the facet on the Rubik's Cube to the fixed numbering shown in Figure 4

7.4 The Illegal Rubik's Cube Group

Now, the possible arrangements of the corner cubes can be described similarly. Again, any of the eight corner cubes can occupy any of the corner cube positions of the Rubik's Cube. So, the possible arrangements of the corner cubes can be described by the permutation group of eight elements, S_8

(ii). The position of all of the corner facets on the Rubik's Cube can be described by the group $8C_3 \wr S_8$

The illegal Rubik's Cube group allows the solver to take the cube apart and reassemble it in any orientation. Again, some of the orientations are not physically possible on the cube. When all the possible positions of the facets are combined as a whole, some of the arrangements will not be physically possible on the cube.

The Illegal Rubik's Cube Group is $I = (12C_2 \wr 12) \times (8C_3 \wr S_8)$

8 Fundamental Theorems of Cube Theory

To be able to distinguish between the legal and illegal Rubik's Cube Group, the First and Second Fundamental Theorems of Cube theory are needed. The First Fundamental Theorem of Cube Theory gives the criteria for solvable arrangements of the Rubik's Cube. The illegal Rubik's Cube group allows the solver to take the cube apart and reassemble it. However, the cube may get re-assembled in an arrangement that is not solvable.

8.1 First Fundamental Theorem of Cube Theory

Let, $v \in 8_{C3}, r \in S_8, w \in 12_{C2}$ and $s \in S_{12}$, then

The 4-tuple (v, r, w, s) corresponds to a arrangement(position) of the cube if and only if

- (1) $\text{sgn}(r) = \text{sgn}(s)$ (equal parity of permutations)
- (2) $v_1 + v_2 + v_3 + \dots + v_8 = 0 \pmod{3}$ (conservation of the total no of twists)
- (3) $w_1 + w_2 + w_3 + \dots + w_{12} = 0 \pmod{2}$ (conservation of the total no of flips)

8.2 Second Fundamental Theorem of Cube Theory

An operation of the cube is possible if and only if the following are satisfied:

- (1) The total number of edge and corner cycles of even length is even.
- (2) The number of corner cycles twisted right is equal to the number of corner cycles twisted left (up to modulo 3).
- (3) There is an even number of reorienting edge cycles.

9 Application of the Legal Rubik's Cube Group

Using the criteria of the First and Second Fundamental Theorems of Cube Theory, the Illegal Rubik's Cube Group can be reduced to the group

$$G_0 = \{v, r, w, s\} : v \in 8_{C3}, r \in S_8, w \in 12_{C2}, s \in S_{12}\}$$

where G_0 has the Properties of First and Second Cube Theorem.

The Illegal Rubik's Cube is Defined to be $I = (12_{C2} \wr 12) \times (8_{C3} \wr S_8)$

However by the conditions of the first theorem, the group is double counting some positions of the facets. The Second Condition of First Cube Theorem determines the position of the corner cubes, but note that once 7 of the corners cubes have their arrangement, the last cube's position would automatically be determined by given formula. Likewise, condition(3) determines the orientation of the cubes.

1. There exists an isomorphism $G_0 \cong (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$

$$\text{and } |G_0| = |S_8| |S_{12}| |11_{C2}| |7_{C3}| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$$

Solution : By the First Cube Theorem, The First Isomorphism Theorem of Groups and the definition of semi-direct product,

$$G_0 \cong (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12}).$$

$$|G_0| = |S_8| |S_{12}| |11_{C2}| |7_{C3}| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$$

Now to obtain the Rubik's Cube group G , G_0 must be further reduced. Condition (1) of First Cube Theory says that the number of even permutation is equal to the odd permutations. So G_0 must be further reduced by a factor of C_2

2. The Rubik's Cube Group G is the kernel of the homomorphism $\phi : G_0 \rightarrow \{1, -1\}$ so that $(v, r, w, s) \mapsto \text{sgn}(r) \text{sgn}(s)$

In particular, $G \subset G_0$ is normal of Index 2 and $|G| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$

Solution : Let, $G_0 = (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$, $H = \{1, 1\}$ and

$\phi : G_0 \rightarrow H$, where $(v, r, w, s) \mapsto \text{sgn}(r) \text{sgn}(s)$.

then $\ker(\phi) = \{v, r, w, s\} : \phi(v, r, w, s) = e_H\}$ where $e_H = 1$.

By First Cube Theorem, The First Isomorphism Theorem of Groups $G_0 / \ker(\phi) \cong G$, where $G_0 = (7_{C3} \wr S_8) \times (11_{C3} \wr S_{12})$.

$$\text{Next, } |G| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7 \text{ and } [G_0 : G] = (8! \cdot 12! \cdot 2^{11} \cdot 3^7) / (8! \cdot 12! \cdot 2^{10} \cdot 3^7) = 2$$

10 Sylow Theorems

M.L Sylow did work of fundamental importance in determining the structure of finite groups. There are two types of groups, i.e. (1) Finite groups, (2) Non Finite groups. Non abelian finite groups are vastly more complicated than finite abelian groups. The Sylow Theorems are the first basic step in understanding the structure of non abelian finite groups. Since the proofs of theorems are largely unrelated to the way the theorems are actually used to analyze groups, so here I'm not giving the proofs. In this section we shall try to give this paper a sound understanding of the meaning of Sylow Theorems and some examples of their application.

Throughout the general discussion in this section all groups are written multiplicatively and all integers are assumed to be nonnegative.

The main theme is the close connection between the structure of a group G and the arithmetic properties of the integer. One of the most important results of this sort is Lagrange's Theorem, which states that if G has a subgroup H , then the order of H divides $|G|$. The First Sylow Theorem provides a particular converse.

Here, we are not discussing conjugacy class, Cauchy's theorem and p -groups because so that the paper does not get bigger.

Now we state three Sylow theorems without proof:

10.1 The First Sylow Theorem

Let G be a group of order $p^n m$ with $n \geq 1$, where p is prime, n, m are positive integers and p, m are relatively prime. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i (i is less than n) is normal in some subgroup of order p^{i+1} .

10.2 The Second Sylow Theorem

Let G be a finite group of order $p^n m$, where p is a prime, n and m are positive integers, and p and m are relatively prime. Then any two Sylow p -subgroups of G are conjugate and therefore isomorphic.

10.3 The Third Sylow Theorem

Let G be a finite group of order $p^n m$, where p is a prime, n and m are positive integers, and p and m are relatively prime. Then the number n_p of Sylow p -subgroup of G is $1 + kp$ for some nonnegative integer k and $n_p \mid p^n m$.

11 Application of Sylow Theorems on Rubik's Cube

According to the Sylow theorems,

there exist subgroups of the cube group of the following orders: $2^{27}, 3^{14}, 5^3, 7^2, 11^1$.

That's because these are the maximal prime powers in the factorization of

$|G| = 43252003274489856000$.

Subgroups of order 11, 49, and 125 are easy to think of:

11: An 11-cycle, i.e.

$\langle (UF UL UB UR DF DL DB DR FL BL BR) \rangle$

49: Two independent 7-cycles, i.e.

$\langle (UF UL UB UR DF DL DB), (UFL UBL UBR UFR DFL DBL DBR) \rangle$

125: Three independent 5-cycles, i.e.

$\langle (UF UL UB UR DF) (DL DB DR FL BL), (UFL UBL UBR UFR DFL) \rangle$

A "3-subgroup" is also not that hard to construct, although now orientation factors in: 4 3-edge cycles, 2 3-edge cycles, 7 corners of CO freedom, which makes 3^{13} . We can also permute three orbits of three-edge-cycles among each other to get up to 3^{14} .

What I'm really wondering about is the group of order 2^{27} . I think I can get it like this (writing it out by hand to give the idea; forgive small errors):

\langle [Flip UF and UL],
 [Flip UF and UB], [Flip UF and UR],
 [Flip UF and DF], [Flip UF and DL],
 [Flip UF and DB], [Flip UF and DR],
 [Flip UF and FL], [Flip UF and BL], [Flip UF and BR], [Flip UF and FR],
 (UF DB), (UL DR), (UB DF), (UR DL), (FL BR), (BL FR), (UF UB) (DB DF),
 (UL UR) (DR DL), (FL FR) (BL BR), (UF UL) (DF DL) (UB UR) (DB DR), (UFL DFL) (UBL DBL) (UBR DBR) (UFL DFL), (UFL UBR), (UBL UFR), (DBR DFL), (DFR DBL), (UFL UBL) (UFR UBR), (DFL DBL) (DFR DBR) \rangle

Which has 28 generators and gives us an illegal group whose even permutations form a subgroup of G of order 2^{27} .

Assuming I got that right, every subgroup of order 2^{27} is conjugate to that, and there are an odd number of such subgroups (Sylow theorems 2 and 3).

12 Concluding Remarks

This paper explored some of the group theory applications to the Rubik's cube and constructed the Rubik's Cube Group. The Rubik's Cube Group was shown to be

$G = \langle F, L, U, D, R, B \rangle$, which is a subgroup of S_{54} . The First and Second Fundamental Theorems of Cube Theory were presented, which gave the criteria for all the possible arrangements and moves allowed on the cube. Defined the Rubik's Cube group to

$$G = (7_{C3} \wr S_8) \times (10_{C2} \wr S_{12})$$

Furthermore the group G was Shown to be the kernel of homomorphism of

$$G_0 = (7_{C3} \wr S_8) \times (10_{C2} \wr S_{12}) \rightarrow \{1, 1\}$$

The Scope of this paper was restricted to the 3x3x3 Rubik's Cube Group; the method developed in this project can be extended to describe group structure of the 4x4x4 and 5x5x5 Rubik's Cube. Moreover, the algorithm for solving any of the 3 cubes can be described in terms of group operations.

13 Reference

- (1). Group Theory and the Rubik's Cube by Lindsey Daniels.
- (2). Group Theory, The dihedral group by Prof. Alexandru Suciu.
- (3). Group Theory, PERMUTATION GROUPS by RAJESH SINGH.
- (4). Introduction to Group Theory and Permutation puzzles.
- (5). <https://www.speedsolving.com/threads/sylow-subgroups-of-the-cube-group.20018>.
- (6). Explorations of Rubik's Cube by zeb Howell.
- (7). Thomas W. Hungerford, Abstract Algebra An Introduction (Third Edition).
- (8). D.S. Malik, John M Mordeson and M.K. Sen, Fundamentals of Abstract Algebra.

Shubhajit Bhowmick

Registration No : A01-1152-113-057-2017

Roll no : 1374

Semester : 5

Paper : CC-12

**Topic : The Framework of Music Theory as
Represented with Groups**

Acknowledgement

I would like to express my special thanks of gratitude to our beloved **Pravanjan Kumar Rana Sir** who gave me the opportunity to do this wonderful project on the topic **The Framework of Music Theory as Represented with Groups**, which also helped me in doing a lot of research and I come to know about so many new things.

Secondly I would like to thank my friends **Pranay Mandal** and **Satyabrata Pradhan** who helped me a lot in finishing this project within the limited. It helped me increase my knowledge and skills.

The Framework of Music Theory as Represented with Groups

Contents

- 1 Introduction
- 2 Basic Group Theory
 - 2.1 What is a group ?
 - 2.2 Permutations
 - 2.3 Morphisms
 - 2.3.1 Homomorphisms
 - 2.3.2 Isomorphisms
 - 2.3.3 Automorphisms
 - 2.4 Products
 - 2.4.1 Direct Products
 - 2.4.2 Semidirect Products
 - 2.4.3 Wreath Products
- 3 Music Theory
 - 3.1 Basic concepts of atonal music theory
 - 3.1.1 T_n , the Transpositions
 - 3.1.2 $T_n I$, the Inversions
- 4 Group Theory as a Structure for Atonal Music Theory
- 5 A Flaw in Atonal Music Theory
- 6 Uniform Triadic Transformations

6.1 Introduction to Triadic Transformations

6.2 V , the Uniform Triadic Transformations

6.2.1 Multiplication on V

6.2.2 Inversion on V

6.2.3 Isomorphism to $Z_{12} \wr Z_2$

6.2.4 Even and Odd UTTs

6.3 R , the Riemannian UTTs

6.4 K , the Subgroups of V

7 Musical Application

8 Conclusion

References

1. Introduction

In 2002, a music theorist by the name of Julian Hook published a paper in the Journal of Music Theory titled, “Uniform Triadic Transformations.” In this paper, Hook generalized some existing music theoretical concepts and greatly improved their notation. Hook’s UTTs formed a group with interesting algebraic properties.

This paper will first give the reader a review of all necessary group theory to understand the discussion of Hook’s UTTs. Then it will review music theory (atonal theory in particular) and its evolution to the UTTs. Finally, it will discuss the UTTs themselves and conclude with some musical applications.

2 . Basic Group Theory

Group theory is a branch of mathematics that studies groups. This algebraic structure forms the basis for abstract algebra, which studies other structures such as rings, fields, modules, vector spaces and algebras. These can all be classified as groups with addition operations and axioms.

This section provides a quick and basic review of group theory, which will serve as the basis for discussions in the group theoretical structure as applied to music theory.

2.1 . What is a group?

A group is a set such that any two elements x and y can be combined via “multiplication” to form a unique product xy that also lies in the set. This multiplication is defined for every group and does not necessarily refer to the traditional meaning of “multiplication.” We now state the formal definition of a group:

Definition 2.1. A group is a set G together with a multiplication on G which satisfies three axioms:

- (a) The multiplication is associative, that is to say $(xy)z = x(yz)$ for any three (not necessarily distinct) elements in G .
- (b) There is an element $e \in G$, called an identity element, such that $xe = e = ex, \forall x \in G$
- (c) Each element $x \in G$ has an inverse x^{-1} which belongs to the set G and satisfies $x^{-1}x = e = xx^{-1}$

Theorem 2.2. Every group G satisfies the following properties:

- (a) The identity element e of G is unique
- (b) $\forall x \in G$, the inverse x^{-1} is unique

Note how commutativity of the multiplication is not required within a group. Therefore, we define an abelian group as follows:

Definition 2.3. A group G is abelian if its multiplication is commutative. That is, $xy = yx$ for any two elements in G .

To better illustrate the concept of a group, we now give some examples. Example 2.4. The reals excluding 0, $\mathbb{R} \setminus \{0\}$ under multiplication:

- The group is closed under multiplication: $\forall x, y \in \mathbb{R}, x \cdot y \in \mathbb{R}$

- The multiplication is associative: $\forall x, y, z \in \mathbb{R}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- The identity is 1: $\forall x \in \mathbb{R}, 1 \cdot x = x \cdot 1$
- The inverse of x is $\frac{1}{x}$: $\frac{1}{x} \cdot x = 1 = x \cdot \frac{1}{x}$

This group is abelian since $x, y \in \mathbb{R}$, $x \cdot y = y \cdot x$. Note how we must exclude 0 for this to be a group since there exists no inverse for 0. That is, there does not exist some $x \in \mathbb{R}$ such that $x \cdot 0 = 1$

Example 2.4. The integers $\mathbb{Z} \pmod{12}$, which we will denote as \mathbb{Z}_{12} , under addition $\pmod{12}$. (Note: in abstract algebra, $\mathbb{Z} \pmod{12}$ is generally notated as $\mathbb{Z}/(12)$ and \mathbb{Z}_{12} refers to another algebraic structure. However, in music theory, only $\mathbb{Z} \pmod{12}$ is of significance and we will use this more concise notation.)

- The group is closed under addition $\pmod{12}$: for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y \in \mathbb{Z}_{12}$.
- Addition $\pmod{12}$ is associative.
- The identity is 0.
- The inverse of x is $12 - x$.

This group is also abelian since for all $x, y \in \mathbb{Z}_{12}$, $x +_{12} y = y +_{12} x$.

Example 2.6. The dihedral groups represent the symmetries of a regular polygon that map it onto itself. Consider the regular hexagon. Let r denote the rotation of through $\pi/3$ about the axis of symmetry perpendicular to the hexagon (rotating), let s denote the rotation through π about an axis of symmetry that lies in the plane of the plate (flipping), and let e denote the identity (leaving the hexagon unchanged). Then the dihedral group D_6 consists of the following 12 elements.

It may seem that the group is not closed under multiplication since the element sr is missing from the group. However, a rotation r takes the hexagon. A subsequent flip s takes the hexagon. Thus, rs is equivalent to r^5s . The reader can check that the whole group is indeed closed under multiplication. In general,

$$sr^n = r^{6-n}s, \forall n \in \mathbb{Z}_6$$

for the D_6 dihedral group.

Definition 2.7. The order of a group is the number of elements in the group.

Definition 2.8. The order of some element x of a group G is the smallest positive integer n such that $x^n = e$.

Definition 2.9. A subgroup of a group G is a subset of G which itself forms a group under the multiplication of G

Definition 2.10. A group G is cyclic if there exists an $x \in G$ such that for all $y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$. We call x a generator of G .

Definition 2.11. A permutation of an arbitrary set X is a bijection from X to itself.

Permutations can be denoted in multiple ways. Consider r from the D_6 dihedral group. We can represent it as a permutation of integers like so: (054321) , where each integer is sent to the one following it, and the final one is sent to the first. Likewise, we can write sr as $(01)(25)(34)$.

Definition 2.12. A permutation of the form $(a_1 a_2 \dots a_k)$ is called a cyclic permutation. A cyclic permutation of length k is called a k -cycle.

Definition 2.13. A transposition is 2-cycle. Any k -cycle $(a_1 a_2 \dots a_k)$ can be written as a product of transpositions:

$$(a_1 a_2 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$$

Note that transpositions may be written as many different products. This product is not unique, but is meant to show the existence of a product consisting only of transpositions.

Definition 2.14. An even permutation is a permutation that can be written as an even number of transpositions. The others are called odd permutations.

It may bother the reader that the a permutation in the form of a product of transpositions is not unique. Perhaps a permutation could be written as both an even number of transpositions and an odd number. However, the following theorem shows that the definition is well defined.

Theorem 2.15. Although any permutation can be written as a product of transpositions in infinitely many different ways, the number of transpositions which occur is always even or always odd.

Theorem 2.16. Consider the set X of n elements. The set of all permutations of X forms a group S_n called the symmetric group of degree n . Multiplication on this group is defined by composition of functions.

2.3 Morphisms

2.3.1 Homomorphisms

Definition 2.17. Let G and G' be groups. A homomorphism is a function $\phi : G \rightarrow G'$ that preserves the multiplication of G . Therefore, $\phi(xy) = \phi(x)\phi(y), \forall x, y \in G$

Example 2.18. Let ϕ be a function from D_{12} to Z_2 defined by $\psi(r^n) = 0$ and $\psi(r^n s) = 1$. Consider two elements x and y in D_{12} . We have four cases:

$$\bullet x = r^m, y = r^n;$$

$$\psi(xy) = \psi(r^m r^n) = \psi(r^{m+n}) = 0 = 0 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n;$$

$$\psi(xy) = \psi(r^m s r^n) = \psi(r^{m-n} s) = 1 = 1 + 0 = \psi(x)\psi(y)$$

$$\bullet x = r^m, y = r^n s;$$

$$\psi(xy) = \psi(r^m r^n s) = \psi(r^{m+n} s) = 1 = 0 + 1 = \psi(x)\psi(y)$$

$$\bullet x = r^m s, y = r^n s;$$

$$\psi(xy) = \psi(r^m s r^n s) = \psi(r^{m-n} ss) = \psi(r^{m-n}) = 0 = 1 + 1 = \psi(x)\psi(y)$$

Hence, ϕ satisfies the properties of a homomorphism.

2.3.2 Isomorphisms

Definition 2.19. An isomorphism is a bijective homomorphism.

Example 2.20. \mathbb{Z}_{12} is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$. Consider the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$(0,0) \quad (0,1) \quad (0,2) \quad (0,3)$$

$$(1,0) \quad (1,1) \quad (1,2) \quad (1,3)$$

$$(2,0) \quad (2,1) \quad (2,2) \quad (2,3)$$

Send each element (x, y) to $4x + y$ and you have \mathbb{Z}_{12}

2.3.3 Automorphisms

Definition 2.21. An automorphism of a group G is an isomorphism from G to G . The set of all automorphisms forms a group under composition of functions, which is called the automorphism group of G and written $\text{Aut}(G)$.

Automorphisms fix the identity and send generators to generators.

Example 2.22. Consider the automorphisms of \mathbb{Z}_4 . There are only two generators in this group: 1 and 3. Therefore, there are only two elements in $\text{Aut}(\mathbb{Z}_4)$: the trivial one, and the one that flips 1 and 3.

2.4 Products

2.4.1 Direct Products

Theorem 2.23. The set $G \times H$ of two groups G and H is a group that consists of the elements (g, h) where $g \in G$ and $h \in H$. Given two elements (g, h) and (g', h') of $G \times H$, multiplication on this group is defined by

$$(g, h)(g', h') = (gg', hh')$$

where the first term, gg' , inherits the multiplication of G , and the second, hh' , inherits the multiplication of H . We call this group the direct product $G \times H$ of G and H .

Proof. Associativity follows from the associativity in both G and H . The identity is (e, e) and the (g^{-1}, h^{-1}) is the inverse of (g, h) .

Example 2.24. Consider $\mathbb{Z}_4 \times \mathbb{Z}_2$. This group has 8 elements: $(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)$.

Multiplication is defined by

$$(x, y) + (x', y') = (x + 4x', y + 2y')$$

2.4.2. Semidirect Products

Theorem 2.25. Suppose we have the groups G, H and the homomorphism $\phi : G \rightarrow \text{Aut}(H)$. Then the “twisted” direct product forms a new group. Its elements are of the form (g, h) with $g \in G$ and $h \in H$ and multiplication is defined by

$$(g, h)(g', h') = (g \cdot \phi(h)(g'), h \cdot h').$$

We call this group the semidirect product of G and H .

Example 2.26. Consider the semidirect product $\mathbb{Z}_4 * \mathbb{Z}_2$. The elements in this group are the same as those in $\mathbb{Z}_4 \times \mathbb{Z}_2$ as listed in Example 2.24.

We need to define ϕ . There are only two automorphisms of \mathbb{Z}_4 as shown in Example 2.22. Let the trivial automorphism be denoted with e and the other with σ . Then, since $\phi: \mathbb{Z}_2 \rightarrow \text{Aut}(H)$, we have $\phi(0) = e$ and $\phi(1) = \sigma$.

Now we can perform multiplication on the group. Consider multiplying the elements $(0, 0)$ and $(1, 0)$. Since $\phi(0) = e$ this multiplication is just like that of the direct product:

$$(0, 0)(1, 0) = (0 + \phi(0)1, 0 + 0) = (0 + e(1), 0 + 0)(1, 0)$$

Now consider the elements $(1, 0)$ and $(0, 1)$.

$$(0, 1)(1, 0) = (0 + \phi(1)(1), 1 + 0) = (0 + \sigma(1), 1 + 0) = (3, 1)$$

2.4.3. Wreath Products

The generalized form of a wreath product $G \wr H$ is too complicated for the scope of this paper. Therefore, we will only consider the special case taking a wreath product with \mathbb{Z}_2 .

Consider the group G . Then $G \wr \mathbb{Z}_2$ is isomorphic to $(G \times G) * \mathbb{Z}_2$. We will discuss this semidirect product in the dihedral notation as in Example 2.27. Thus, let the elements of $G \times G$ be denoted by $r_1^m r_2^n$.

The automorphism for a wreath product must permute the parts of an element in $G \times G$. Since we only have two elements, r_1^m and r_2^n , the only non-trivial automorphism is to switch them. That is $\delta(r_1^m r_2^n) = r_2^n r_1^m$. Thus,

$$r_1^m r_2^n s = s \delta(r_1^m r_2^n) = s r_2^n r_1^m$$

3. Music Theory

Music theory is a tool and framework with which we explain our listening experience. However, both the tool and the term “listening experience” are loosely defined. They are dependent on the music.

During the mid-15th century, composers began constructing their pieces around a particular pitch, called the tonic. This pitch was quickly established at the start of the piece and all other pitches were heard relative to it. Intervals and chords were labeled as consonant or dissonant. A feeling of tension occurred in various ways, such as when resolution was delayed, or when the music leapt to

distant keys (more than two accidentals removed from the tonic). Resolution to the tonic was crucial to ending the piece. After over two centuries of tonal music, listeners have begun to expect music to resolve in particular ways.

Along with the development of tonal music was the development of tonal theory. Its structure and notation allowed theorists to describe the listener's expectation. Thus, it provided an explanation for our reaction to particular harmonies. It explained our feeling of surprise at a particular chord and our feeling of finality at the end of a piece.

Around the turn of the 19th century, composers pushed the boundaries of tonal music. They began using dissonant chords with unprecedented freedom and resolved them in new ways. Eventually, their pieces no longer fit the framework of tonal music. Tonal theory no longer provided an adequate explanation for our listening experience. Thus, a new framework was constructed called atonal music theory.

Discussions in music require a certain vocabulary. The following terms are defined in the appendix:

- interval
- half step (semitone) & whole step (whole tone), flat, sharp, natural & accidental
- enharmonic equivalence
- major, minor, mode
- parallel & relative
- scale degree
- triad

3.1. Basic concepts of atonal music theory

Atonal music is based on sequences of pitches and intervals. No particular pitch is considered more important than the others and resolution of dissonance is unimportant. It assumes octave and enharmonic equivalence.

Definition 3.1. Pitches that are separated by an integer multiple of an octave, or are enharmonically equivalent belong to the same pitch class.

Definition 3.2. Consider the pitches a and b . The ordered pitch-class interval from a to b is $a-b \pmod{12}$.

Definition 3.3. A pitch-class set is an unordered set of pitch-classes, denoted as a string of integers enclosed in brackets. Within a pitch-class set, we do not have information about the register, rhythm or order of the pitches.

Example 3.4. The C major triad consists of the notes C, E and G. This can be represented as the pitch-class set [047], since $C = 0$, $E = 4$ and $G = 7$.

In atonal music, operations are performed on pitch-class sets, creating new pitch-class sets that are spread throughout the music. Thus, the music sounds random and yet structured at the same time. We will discuss two types of operations in this paper: the transpositions and the inversions.

3.1.1 T_n , the Transpositions

Definition 3.5. The transposition T_n moves a pitch-class or pitch-class set up by $n \pmod{12}$. (Note: moving down by n is equivalent to moving up by $12-n$.)

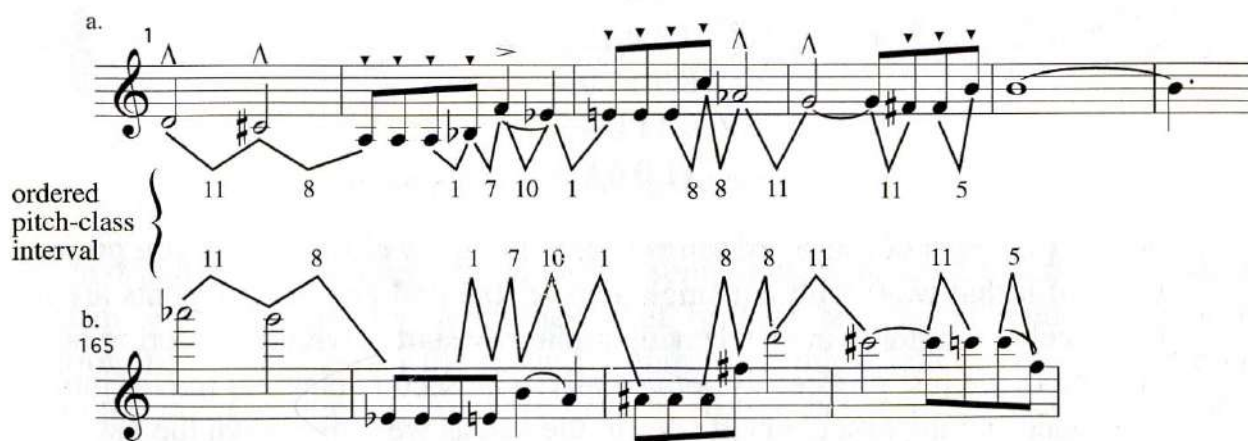


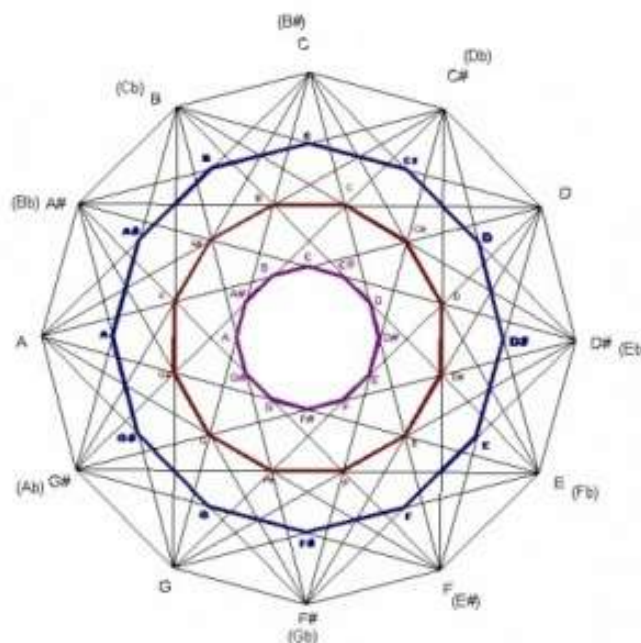
Figure 1: Two lines of pitch classes related by T6 (Schoenberg, String Quartet No. 4).

3.1.2 TnI, the Inversions

Definition 3.6. Consider the pitch a . Inversion $T_n I$ inverts the pitch about $C(0)$ and then transposes it by n . That is, $T_n I(a) = -a + n(\text{mod } 12)$.

4. Group Theory as a Structure for Atonal Music Theory

The numbering of the pitch classes reveals their isomorphism to \mathbb{Z}_{12} . More interestingly, the group of transpositions and inversions, denoted $T_n/T_n I$ is isomorphic to the dihedral group D_{12} .



Sehr langsam $\text{♩} = \text{ca. } 40$

Fl. 1 5

Ob.

Cl. 3

Trp. 1 Immer mit Dmpf. pp

Vln. 2 mit Dmpf. p

Vla. pp

Piano pp p pp 4

1 2 3 4

Figure 3: Transpositionally equivalent pitch-class sets (Webern, Concerto for Nine Instruments, Op. 24).

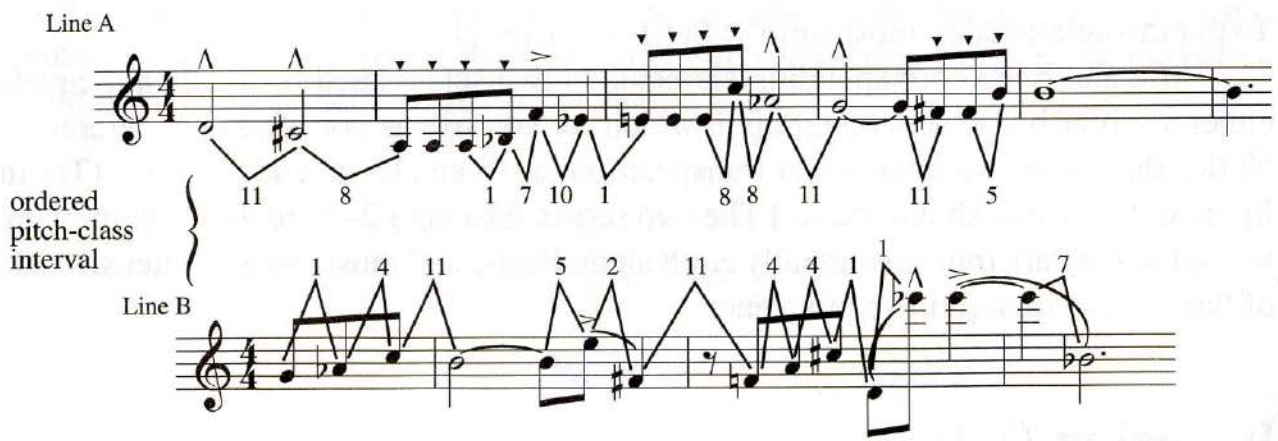


Figure 4: Two lines of pitch classes related by T9I (Schoenberg, String Quartet No. 4)

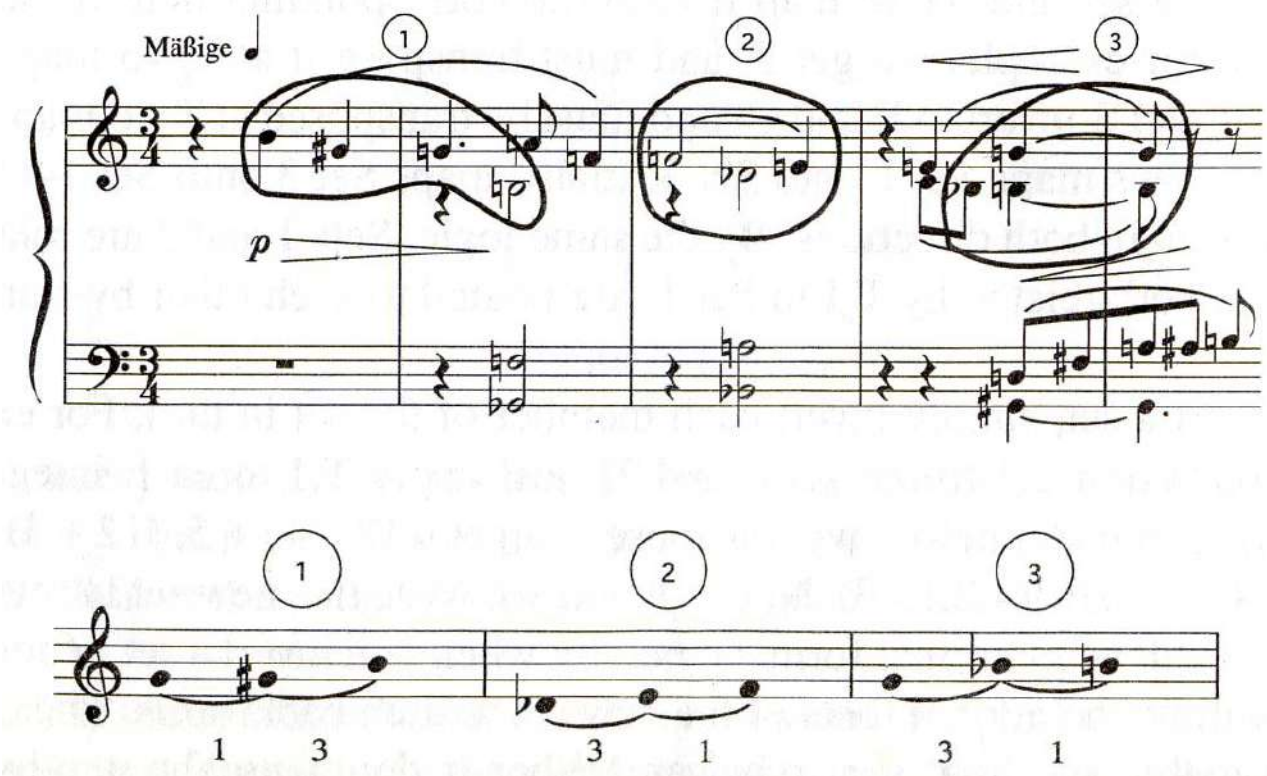


Figure 5: Inversionally equivalent pitch-class sets (Schoenberg, Piano Piece, Op. 11, No. 1)

5. A Flaw in Atonal Music Theory

Consider the operation that changes a major triad to a minor triad. To our ears, this is the same operation regardless of whether we start with a CM triad or a DM triad. However, consider the CM triad as the pitch class [047], cm as [037], DM as [269] and dm as [259]. Then, we have

$$\text{CM} \rightarrow \text{cm} = [047] \rightarrow [037] = \text{T7I} \quad \text{DM} \rightarrow \text{dm} = [269] \rightarrow [259] = \text{T11I}$$

This is a misleading representation of the music, because our ears do not hear two different actions. Therefore, the structure of atonal music theory has an inherent flaw. It cannot support these simple transformations.

A music theorist named Hugo Riemann recognized this problem. He invented the idea of a “triadic transformation.” Later music theorists devised three operations, called Neo-Riemannian operations, that functioned specifically on triads:

- The Parallel operation (P) moves the middle note of a triad up or down a semitone such that a major triad becomes minor and a minor triad becomes major. For example, it would move the E in a CM to an E \flat and the E \flat in a cm triad to an E \natural .
- The Leading-tone exchange (L) moves the bottom note of a major triad down a semitone and the top note of a minor triad up a semitone. Thus, a CM triad would turn into an em triad, and a cm triad would turn into an A \flat M triad.
- The Relative operation (R) sends a chord to its relative counterpart by moving the top note of a major triad up by a whole tone, and moving the bottom note of a minor triad down by a whole tone. Thus, a CM triad would turn into an am triad, and a cm triad would turn into an E \flat M triad.

These three were particularly interesting because they allowed for parsimonious voice-leading. That is, in moving from one triad to another, only one voice (top, middle or bottom) moved, and it moved by nothing more than a whole step. In addition, they allowed a transformation from any one chord to another by composition of these operations.

6. Uniform Triadic Transformations

This P, L and R notation, while a definite improvement, could still be unclear, unwieldy and limited in its usefulness. For example, a move from a CM triad to a b \flat m triad requires a minimum of six Neo-Riemannian operations. Furthermore, there are nine different ways to write it in six operations: LPRPR, LRPRP, PLRLR, PRLRP, PRPRL, RLPLR, RLRLP, RPLPR, RPRPL. Of course, there are even more ways to write it in more than six operations. Not only has this notation become pedantic, it also fails to reflect the music: who would hear six operations in a simple move from CM to b \flat m?

To resolve this problem, another music theorist named Julian Hook devised a new notation for transformations on triads, which he called uniform triadic transformations (UTTs). This notation, in fact, was a group structure with intriguing algebraic properties. Before we jump into a discussion on

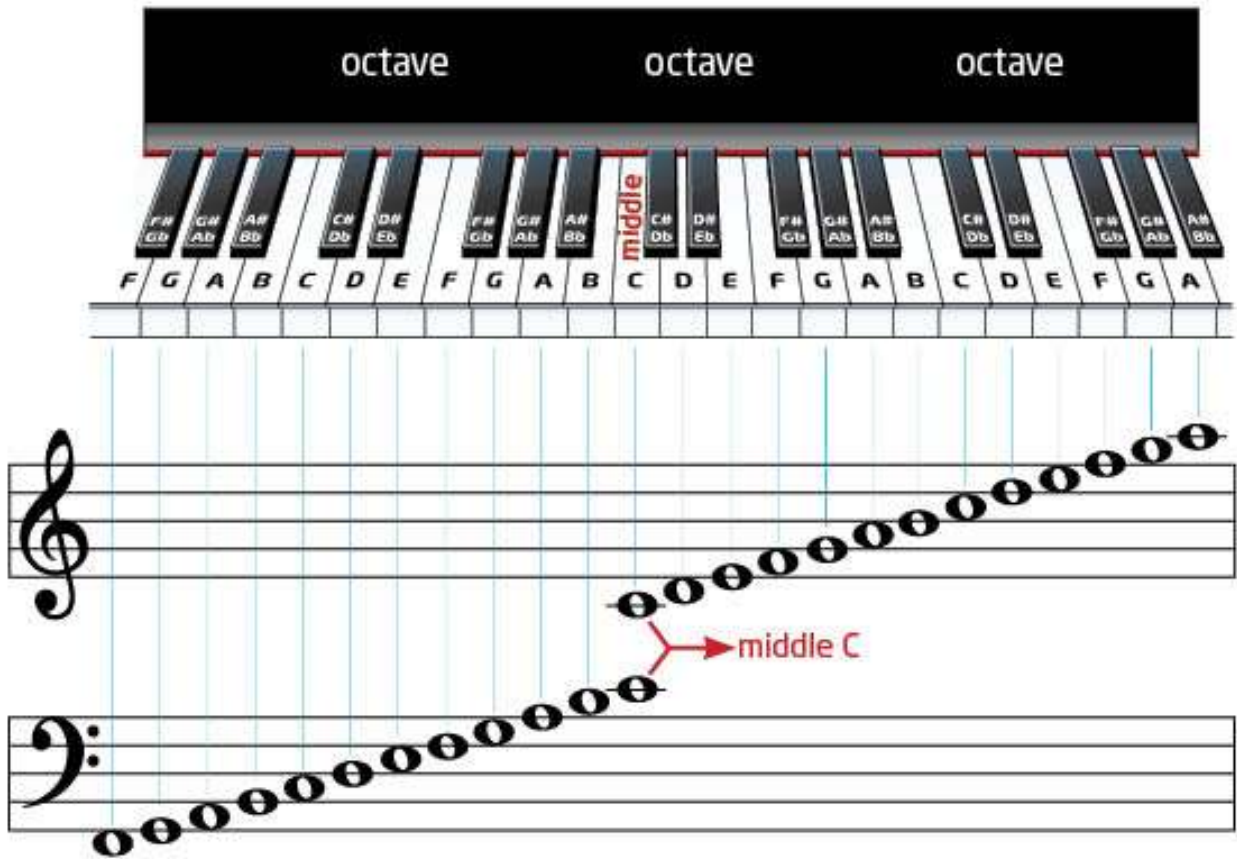


Figure 6: A piano with the keys placed onto the music staff

Definition 6.1. A triad is an ordered pair $\Delta = (r, \sigma)$ where r is the root of the triad expressed as an integer (mod 12), and σ is a sign representing its mode (+ for major, - for minor).

Example 6.2. $\Delta = (0, +)$ represents a C major triad and $\Delta = (6, -)$ represents an f# minor triad.

Theorem 6.3. The set of all 24 major and minor triads, forms a abelian group with multiplication defined by

$$(t_1, \delta_1)(t_2, \delta_2) = (t_1 + t_2, \delta_1\delta_2)$$

We call this set Γ .

Proof. This group is clearly isomorphic to $\mathbb{Z}_{12} \times \mathbb{Z}_2$, which by Theorem 2.23 is a group.

Definition 6.4. Given $\Delta_1 = (r_1, \delta_1)$ and $\Delta_2 = (r_2, \delta_2)$, the transposition level $t = r_2 - r_1$ is the interval between the roots and the sign factor $\delta = \delta_1\delta_2$ is the change in sign. (δ is multiplied as expected with $++ = +, +- = -, -+ = -$ and $-- = +$.) The Γ -interval $\text{int}(\Delta_1, \Delta_2)$ is the ordered pair (t, δ) where t and δ are the transposition level and sign factor as defined above.

Example 6.5. The Γ -interval from $(0, +)$ (C major) to $(6, -)$ (f# minor) is $(6, -)$.

6.1. Introduction to Triadic Transformations

Definition 6.6. A triadic transformation is a bijective mapping from Γ to itself. In other words, it is a permutation of Γ .

Theorem 6.7. The set of all triadic transformations forms a group G . Proof. After numbering the triads, this group is clearly isomorphic to S_{24} .

The order of G is huge: 24 factorial. However, most of these transformations have little musical meaning since the action of a transformation on one triad may not resemble its action on another triad.

6.2. V, the Uniform Triadic Transformations

Of particular musical interest are the UTTs because they operate on all major triads in the same manner. Similarly, the UTTs have one action for all minor triads.

Definition 6.8. Consider the triadic transformation that transforms (r, σ) to (r', σ') . It is a uniform triadic transformation (UTT) if it transforms $(r + t, \sigma)$ to $(r' + t, \sigma')$ $\forall t \in \mathbb{Z}_{12}$.

It is important to note that not all musically interesting transformations are UTTs. The inversions TnI , for example, are not part of the UTTs.

Any UTT is completely determined by three parameters:

- t^+ , its transposition level for a major triad
- t^- , its transposition level for a minor triad
- σ , its sign. (Note: it may seem that σ could be different for major and minor triads. However, in order to be a transformation, a UTT must map Γ to itself. Thus, if it switches major triads to minor, it must switch minor triads to major. That is $\delta^+ = -\delta^-$. Positive σ implies no change in mode (it is **mode-preserving**), negative σ implies switching to the opposite mode (it is **mode-reversing**).)

We can thus denote any UTT U by the ordered triple $U = \langle \sigma, t^+, t^- \rangle$. Example 6.9. We will convert Riemann's P, L and R in UTT notation:

$$P = \langle -, 0, 0 \rangle \quad L = \langle -, 4, 8 \rangle \quad R = \langle -, 9, 3 \rangle$$

Note, Hook uses left-to-right orthography. Thus, $U_1 U_2$ implies “first U_1 then U_2 .” As usual, $U^2 = U U$, etc. Although it is less intuitive for mathematicians, we will adhere to his notation.

6.2.1 Multiplication on V

Multiplication on V should clearly be composition. Before we derive a general formula for the composition of two UTTs, let us consider some concrete examples.

Example 6.10. Consider the UTTs $U = \langle +, 4, 7 \rangle$ and $V = \langle -, 5, 10 \rangle$. Let us calculate the product $UV = \langle \delta_{UV}, t_{UV}^+, t_{UV}^- \rangle$. When UV acts on a CM triad ($\Delta = (0, +)$) we have:

$$(0, +) \xrightarrow{U} (4, +) \xrightarrow{V} (9, -)$$

Thus, UV transforms the major triads through the Γ -interval (9, -). We can deduce that $\delta_{UV} = -$ and $t_{UV}^+ = 9$.

When UV acts on a cm triad ($\Delta = (0, -)$) we have:

$$(0, -) \xrightarrow{U} (7, -) \xrightarrow{V} (5, +)$$

Thus, UV transforms the minor triads through the Γ -interval (5, +) and $t_{UV}^- = 5$. Hence, $UV = \langle -, 9, 5 \rangle$

This product may be calculated by multiplying the signs ($\delta_{UV} = \delta_U \delta_V$) and adding the corresponding transposition levels ($t_{UV}^+ = t_U^+ + t_V^+$; $t_{UV}^- = t_U^- + t_V^-$). Figure 6 depicts a visual representation of UV.

Example 6.11. Now consider the product VU. In this case we have

$$(0, +) \xrightarrow{V} (5, -) \xrightarrow{U} (0, -)$$

and

$$(0, -) \xrightarrow{V} (10, +) \xrightarrow{U} (2, +)$$

Therefore, $VU = \langle -, 0, 2 \rangle$. In this case, the signs were multiplied as before, the transposition levels were “cross-added.” That is, $t_{UV}^+ = t_U^+ + t_V^-$ and $t_{UV}^- = t_V^+ + t_U^-$.

We can see that in the above example, the “cross-adding” was due to the sign of the first transformation. In the first case, the first UTT (U) was mode-preserving, so the second UTT (V) acted on the same mode as U. Thus, the corresponding transposition levels were applied in succession. In the second case, the first UTT (V) was mode-reversing, so the second UTT (U) acted on the opposite mode as V and opposite transposition levels were combined. This leads us to the general form of UTT multiplication:

Theorem 6.12. Consider two UTTs $U = \langle \delta_U, t_U^+, t_U^- \rangle$ and $V = \langle \delta_V, t_V^+, t_V^- \rangle$. Multiplication on V is given by $UV = \langle \delta_U \delta_V, t_U^+ + t_V^{(\delta_U)}, t_U^- + t_V^{(-\delta_U)} \rangle$

The reader can verify that following the process above using two arbitrary elements in V will give the desired result.

6.2.2 Inversion on V

Again, before we derive a general formula for the inverse of a UTT, let us consider some concrete examples.

Example 6.13. Consider the UTT $U = \langle +, 4, 7 \rangle$. Because $(0, +) \xrightarrow{U} (4, +)$ and $(0, -) \xrightarrow{U} (7, -)$, we need $(4, +) \xrightarrow{U^{-1}} (0, +)$ and $(7, -) \xrightarrow{U^{-1}} (0, -)$. Thus, $U^{-1} = \langle +, 8, 5 \rangle$. Note how this is simply the inversion of the transposition levels: $\langle +, -4 \pmod{12}, -7 \pmod{12} \rangle$.

Example 6.14. Now consider the UTT $V = \langle -, 5, 10 \rangle$. $(0, +) \xrightarrow{V} (5, -)$ and $(0, -) \xrightarrow{V} (10, +)$. Thus, $(5, -) \xrightarrow{V^{-1}} (0, +)$ and $(10, +) \xrightarrow{V^{-1}} (0, -)$. Therefore, $V^{-1} = \langle -2, 7 \rangle$ or $\langle -, -10 \pmod{12}, -5 \pmod{12} \rangle$. In this case, the transposition levels are not only inverted, but interchanged. Once again, this is due to the sign of V .

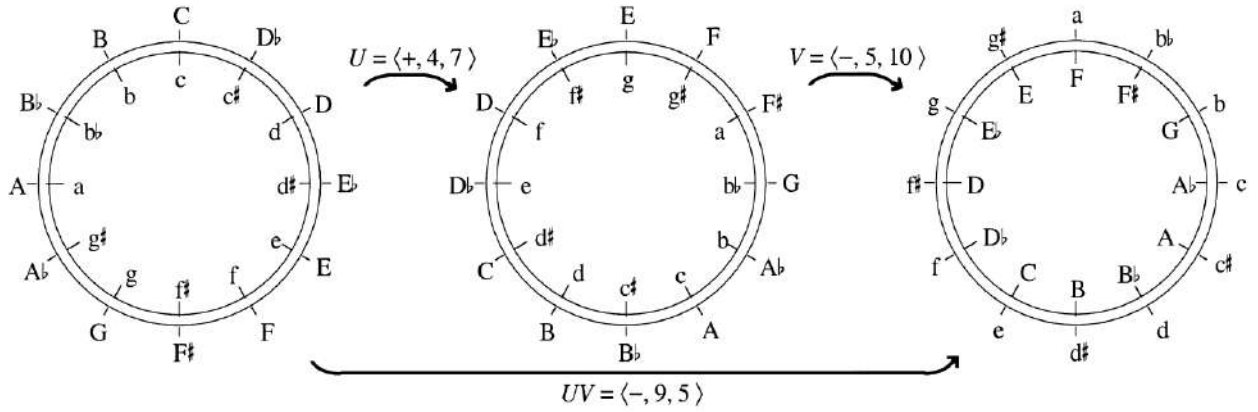


Figure 7: Visual representation of the UTT equation $\langle +, 4, 7 \rangle \langle -, 5, 10 \rangle = \langle -, 9, 5 \rangle$

Theorem 6.16. The set V of UTTs is a group that is isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$

Proof. Remember from Section 2.4.3 how we represented $G \times G$ in the form $r_1^m r_2^n$. Let G be \mathbb{Z}_{12} and let us switch the 1 and 2 to + and -. Then the elements of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ are $s r_+^m r_-^n$ where $m, n \in \mathbb{Z}_{12}$.

Also note that the transpositions, which are equivalent to the transposition levels of a UTT, are isomorphic to the rotations of the D_{12} by $T_n \rightarrow r^n$. We initially wrote that the $T_n/T_n I$ group was isomorphic by $T_n \rightarrow r^{12-n}$. This reflected our visual representation of the two groups. However, the groups are still isomorphic if we choose $T_n \rightarrow r^n$, which makes the following argument clearer.

It seems likely that the UTTs are isomorphic to $\mathbb{Z}_{12} \wr \mathbb{Z}_2$ by $\langle \sigma, t^+, t^- \rangle \rightarrow s r_+^m r_-^n$. We have already shown that the UTTs have multiplication and inverses. We only need to show that it follows the multiplication of $\mathbb{Z}_{12} \wr \mathbb{Z}_2$. That is, $(r_+^m r_-^n)s = s(r_-^n r_+^m)$.

$$\begin{aligned}
 (r_+^m r_-^n)s &= (e r_+^m r_-^n)(see) \\
 &= \langle -, 0, 0 \rangle \langle +, t_m^+, t_n^- \rangle \\
 &= \langle -, 0 + t_n^-, 0 + t_m^+ \rangle \\
 &= \langle -, t_n^-, t_m^+ \rangle \\
 &= s(r_-^n, r_+^m)
 \end{aligned}$$

Thus, multiplication is preserved and the isomorphism holds.

6.2.3 Even and Odd UTTs

UTTs can be classified as “even” or “odd” in multiple ways. Let us begin with “even/odd in the sense of total transposition.”

Definition 6.17. We say that a UTT $U = \langle \sigma, t^+, t^- \rangle$ is even (or, more fully, even in the sense of total transposition) if its total transposition $\tau(U) = t^+ + t^-$ is an even number. U is odd (in the sense of total transposition) if $\tau(U)$ is an odd number.

Definition 6.19. A UTTs is even (in the sense of permutation theory) if it can be written as a product of an even number of 2-cycles and odd (in the sense of permutation theory) if it can be written as a product of an odd number of 2-cycles.

It is remarkable that the two definitions of even or odd (in the sense of total transposition versus permutation theory) are actually equivalent.

Theorem 6.20. A UTT is even in the sense of total transposition if and only if it is even in the sense of permutation theory.

6.3. \mathbb{R} , the Riemannian UTTs

Recall the Neo-Riemannian operators P , L and R as introduced in Section 5 and written as UTTs in Example 6.9. For each, the transposition level for a major triad is equal and opposite that of a minor triad. We define the Riemannian UTTs as follows.

Definition 6.21. A Riemannian UTT is a UTT such that $t^+ = -t^-$.

Theorem 6.22. The set of \mathbb{R} of Riemannian UTTs is isomorphic to D_{12} .

Proof. D_{12} can be defined as the group of order 24 generated by s and r , such that $s^2 = e$, $r^{12} = e$ and $sr = r^{-1}s$

The generators of \mathbb{R} are $\langle -, 0, 0 \rangle$ and $\langle +, 1, 11 \rangle$.

$$(\langle -, 0, 0 \rangle)^2 = \langle -, 0+0, 0+0 \rangle = \langle +, 0, 0 \rangle = e \in \mathbb{R}$$

$$(\langle +, 1, 11 \rangle)^{12} = \langle +, 12 \cdot (1), 12 \cdot (11) \rangle = \langle +, 0, 0 \rangle = e$$

$$(\langle +, 1, 11 \rangle)^{-1} = \langle +, 11, 1 \rangle$$

$$\langle -, 0, 0 \rangle \langle +, 1, 11 \rangle = \langle -, 0 + 11, 0 + 1 \rangle = \langle -, 11 + 0, 1 + 0 \rangle$$

$$= \langle +, 1, 11 \rangle \langle -, 0, 0 \rangle = r^{-1}s$$

6.4 \mathbb{K} , the Subgroups of \mathbb{V}

Generally, it is difficult to list all the subgroups of a given group G . However, it is possible to list all the subgroups of \mathbb{V} .

Definition 6.23. Give two integers a and b (mod 12), we define three subsets of \mathbb{V} as follows.

- $K^+(a)$ is the set of all mode-preserving UTTs of the form $\langle +, n, an \rangle$ as n ranges through the integers mod 12.

- $K^-(a, b)$ is the set of all mode-reversing UTTs of the form $\langle -, n, an+b \rangle$.
- $K(a, b) = K^+(a) \cup K^-(a, b)$

Theorem 6.24. $K(a, b)$ is a subgroup of V if and only if the numbers a and b satisfy $a^2=1$ and $ab = b \pmod{12}$.

The condition $a^2 = 1$ is satisfied only for $a = 1, 5, 7$ and 11 . If $a = 1$ then the condition $ab = b$ is automatically satisfied. For other values of a , the allowable values of b are different in each case. The following is a complete list of the groups $K(a, b)$:

$K(1,0), K(1,1), K(1,2), \dots, K(1,11)$
 $K(5, 0), K(5, 3), K(5, 6), K(5, 9)$
 $K(7, 0), K(7, 2), K(7, 4), K(7, 6), K(7, 8), K(7, 10) K(11, 0), K(11, 6)$

7. Musical Application

The UTTs of order 24 are of considerable musical interest. When such a transformation is applied repeatedly, the resulting chain of triads will cycle through all 24 major and minor triads before returning to the original one. Take, for example, the UTT $U = \langle -, 9, 8 \rangle$. Its repeated application produces a chain in the scherzo of Beethoven's Ninth Symphony :

$$C \xrightarrow{U} a \xrightarrow{U} F \xrightarrow{U} d \rightarrow \dots \xrightarrow{U} A$$

This chain is 19 triads long, only five short of a complete cycle.

Such triad chains are rarely prolonged to this extent. There are, however, examples from literature that circumnavigate the entire cycle of 24 triads. These are found in collections of pieces such as Bach's Well-Tempered Clavier and the Chopin Preludes.

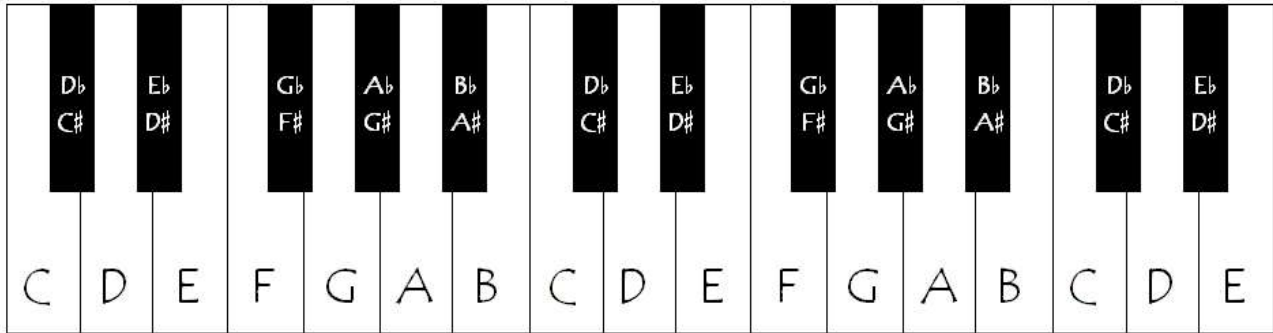


Figure 8: A piano with the keys labeled

8. Conclusion

We can see that Hook's UTTs not only have interesting mathematical properties, but also musical significance. Musically, the choice of triads is non-arbitrary since triads occur throughout music. Mathematically, however, the set choice is arbitrary. Some current research in music theory investigates the generalization Hook's UTTs to larger chords or even to pitch-class sets. The flexibility these generalisations will provide may greatly improve atonal analysis.

References

- [1] Armstrong, M. Groups and Symmetry. Springer-Verlag, 1988.
- [2] Dummit, D. S., and Foote, R. M. Abstract Algebra, third ed. Wiley, 2003.
- [3] Hook, J. Uniform triadic transformations. *Journal of Music Theory* 46, 1-2 (2002), 57–126.
- [4] Straus, J. N. Introduction to Post-Tonal Theory, second ed. Prentice-Hall, Inc., 2000.

Name :- Smigdhadip Chowdhury

Reg. No. :- A01-1122-113-057-2018

Sem :- 5th , Paper Code :- MTMA CE - XII

College Roll No. :- 2368

Topic :- Assignment on Group Theory (II)

1) Let, G be a group. Then $\text{Inn}(G) \triangleleft \text{Aut}(G)$

$$\Rightarrow \text{Inn } G = \{ \theta_a : a \in G \} \quad \text{For any } a \in G, \quad \theta_a(b) = aba^{-1} \quad \forall b \in G$$

Let, $\alpha \in \text{Aut}(G)$ For any $a \in G$, $\theta_a \in \text{Inn}(G)$

$$\begin{aligned} \therefore \alpha \circ \theta_a \circ \alpha^{-1}(b) &= \alpha[a \cdot \alpha^{-1}(b) \cdot a^{-1}] \\ &= \alpha(a) [\alpha(\alpha^{-1}(b))] \alpha(a^{-1}) \\ &= \alpha(a) b \alpha(a^{-1}) \\ &= \alpha(a) b [\alpha(a)]^{-1} \\ &= \theta_{\alpha(a)} b \in \text{Inn}(G) \quad [\because \alpha(a) \in G] \end{aligned}$$

Now, b is an arbitrary element of G and θ_a is an arbitrary element of $\text{Inn}(G)$, α is an arbitrary element of $\text{Aut}(G)$.

$$\therefore \alpha \circ \text{Inn}(G) \circ \alpha^{-1} \subseteq \text{Inn}(G) \quad \forall \alpha \in \text{Aut}(G)$$

$$\therefore \text{Inn}(G) \triangleleft \text{Aut}(G) \quad (\text{Proved}) //$$

2) Let, G be a group and $H < G$ [H is a subgroup of G]
Then, $\frac{N(H)}{C(H)} \cong$ a subgroup of $\text{Aut}(H)$

$$\Rightarrow \text{Where, } N(H) = \{ x \in G : xHx^{-1} = H \} \quad [\text{Normalizer of } H]$$

$$C(H) = \{ x \in G : xh = hx \quad \forall h \in H \} \quad [\text{Centralizer of } H]$$

$$\Rightarrow \text{Let, } \psi : N(H) \rightarrow \text{Aut}(H) \text{ s.t. } \psi(x) = \theta_{x|H}$$

$$\text{Now, } \psi(x_1 x_2) = \theta_{x_1 x_2|H} = \theta_{x_1|H} \circ \theta_{x_2|H} \quad (\text{P.T.O})$$

$$\begin{aligned} \therefore \theta_{x_1 x_2 | H} &= x_1 x_2 H(x_1 x_2)^{-1} = x_1 (x_2 H x_2^{-1}) x_1^{-1} = x_1 \theta_{x_2 | H} x_1^{-1} \\ &= \theta_{x_1 | H} \circ \theta_{x_2 | H} \\ &= \psi(x_1) \circ \psi(x_2) \end{aligned}$$

$\therefore \psi$ is well defined and

ψ is a homomorphism from G to $\text{Aut}(G)$.

$$\begin{aligned} \ker \psi &= \{x \in N(H) : \psi(x) = i_H\} \\ &= \{x \in N(H) : \theta_{x|H}(b) = i_H(b) \quad \forall b \in H\} \\ &= \{x \in N(H) : xbx^{-1} = b \quad \forall b \in H\} \\ &= \{x \in N(H) : xb = bx \quad \forall b \in H\} \\ &= C(H) \end{aligned}$$

Now, By first isomorphism theorem, $\frac{N(H)}{\ker \psi} \cong$ The homomorphic image of $N(H)$

$\Rightarrow \frac{N(H)}{C(H)} \cong$ A subgroup of $\text{Aut}(H)$ (Proved)

④ For $H = G$, $N(G) = G$, $C(G) = Z(G)$ if we had made the same similar mapping $\psi(x) = \theta_{x|G} = \theta_x \left[\psi : G \rightarrow \text{Aut}(G) \right]$

then, the homomorphic image is clearly equal to $\text{Inn}(G)$. [Means ψ is an epimorphism from $G \rightarrow \text{Inn}(G)$]

So, we get

$$\frac{G}{Z(G)} \cong \text{Inn}(G). \text{ (Proved).}$$

4) Show that $\frac{4\mathbb{Z}}{12\mathbb{Z}} \simeq \mathbb{Z}_3$

\Rightarrow Let $f: 4\mathbb{Z} \rightarrow \mathbb{Z}_3$ s.t. $f(4n) = [n] \quad \forall 4n \in 4\mathbb{Z}$

$$\therefore \text{Ker } f = \left\{ 4x \in 4\mathbb{Z} : f(4x) = [0] \right\} \quad \left| \quad \begin{array}{l} \forall [n] \in \mathbb{Z}_3 \exists 4n \in 4\mathbb{Z} \\ \text{s.t. } f(4n) = [n] \end{array} \right.$$

$$= 12\mathbb{Z}$$

By first isomorphism theorem,

$$\frac{4\mathbb{Z}}{\text{Ker } f} \simeq \mathbb{Z}_3$$

$\therefore f$ is an epimorphism from $4\mathbb{Z}$ to \mathbb{Z}_3 .

$$\Rightarrow \frac{4\mathbb{Z}}{12\mathbb{Z}} \simeq \mathbb{Z}_3 \quad (\text{Proved})$$

* If $\text{gcd}(m, n) = 1$ then if we had defined f mapping $f: m\mathbb{Z} \rightarrow \mathbb{Z}_n$ s.t. $f(mx) = [x] \quad \forall mx \in m\mathbb{Z}$ then, $\text{Ker } f = mn\mathbb{Z}$ and if $m > n$ then, f would be an epimorphism from $m\mathbb{Z}$ to \mathbb{Z}_n . And by similarly, $\frac{m\mathbb{Z}}{mn\mathbb{Z}} \simeq \mathbb{Z}_n$ [Example: $\frac{8\mathbb{Z}}{56\mathbb{Z}} \simeq \mathbb{Z}_7$]

5) Prove that $\text{Aut}(\mathbb{Z}_n) \simeq U_n$

\Rightarrow Let, $\phi: \text{Aut}(\mathbb{Z}_n) \rightarrow U_n$ s.t. $\phi(f) = f([1])$

So, we can clearly see that, $m \cdot f([1]) = f([m]) \quad \forall f \in \text{Aut}(\mathbb{Z}_n)$

Now, $|f([m])| = n$ iff $\text{gcd}(m, n) = 1$

$\therefore |f([1])| = n \quad \forall n \in \mathbb{N} \quad \therefore f([1]) \in U_n \quad \forall f \in \text{Aut}(\mathbb{Z}_n)$

$\therefore f$ is well defined.

Now, let $f, g \in \text{Aut}(\mathbb{Z}_n)$ So, $\alpha(f \circ g) = f \circ g([1])$. [Let, $g([1]) = [k]$]
 $= f([k])$

$$\text{Ker } \alpha = \{f \in \text{Aut}(\mathbb{Z}_n) : \alpha(f) = [1]\}$$

$$= \{f \in \text{Aut}(\mathbb{Z}_n) : f([1]) = [1]\}$$

$$= i \quad [i = \text{The identity mapping}]$$

$\therefore \alpha$ is a monomorphism.

$$= kf([1])$$

$$= f([1]) \circ g([1])$$

$$= \alpha(f) \circ \alpha(g)$$

$\therefore \alpha$ is a homomorphism from

$$\text{Aut}(\mathbb{Z}_n) \rightarrow U_n$$

Now, we have to see that α is a surjection from $\text{Aut}(\mathbb{Z}_n)$ to U_n also.

Let, ~~$t \in \mathbb{N}$ s.t.~~ $[t] \in \mathbb{Z}_n$ s.t. $\gcd(t, n) = 1$, ~~$[t] \in U_n$~~
 $\therefore [t] \in U_n$.

Let, $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ s.t. $f([m]) = [mt] \quad \forall [m] \in \mathbb{Z}_n$

f is a homomorphism. $\because f([m+n]) = [m+n]t = [mt] + [nt]$

If in \mathbb{Z}_n , $[r] = [s]$ then $n \mid r-s$

$$\Rightarrow r-s = nq \quad [\text{for some } q \in \mathbb{Z}]$$

$$\Rightarrow rt - st = nqt$$

$$\Rightarrow [rt] = [st]$$

again, for $[rt] = [st]$ then, $n \mid (rt - st)$

$$\Rightarrow n \mid (r-s)t \Rightarrow n \mid (r-s) \quad \left[\because \gcd(n,t)=1, \right. \\ \left. \text{So, } n \nmid t \right]$$

~~$\therefore f$ is an isomorphism from \mathbb{Z}_n to \mathbb{Z}_n .~~

$\therefore f$ is injective from \mathbb{Z}_n to \mathbb{Z}_n .

⊗

$\therefore \alpha$ is an isomorphism from $\text{Aut}(\mathbb{Z}_n)$ to U_n s.t.

$$\alpha(f([1])) = [t] \quad \forall f \in \text{Aut } \mathbb{Z}_n$$

⊗ Let, $[r] \in \mathbb{Z}_n$. Now, $\gcd(n,t)=1$ so, $\exists p, q \in \mathbb{Z}$ s.t.

$$np + qt = 1 \Rightarrow r \equiv r[np + qt]$$

$$\Rightarrow [r] = [rqt] \quad \left[\because \text{In } \mathbb{Z}_n, [rp + n] = 0 \right]$$

$$\therefore \forall [r] \in \mathbb{Z}_n \exists [qt] \in \mathbb{Z}_n \text{ s.t. } f([qt]) = [r] \\ = f([qrt]) \\ = [r]$$

$\therefore f$ is surjective too. $\therefore f$ is an ~~isomorphism~~ automorphism on \mathbb{Z}_n .

$$\therefore f \in \text{Aut}(\mathbb{Z}_n).$$

6) Show that,
 $\text{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$

\Rightarrow We know, $\text{Aut}(\mathbb{Z}_n) \cong U_n \quad \forall n \in \mathbb{N}$

$$\therefore \text{Aut}(\mathbb{Z}_5) \cong U_5$$

Now, $U_5 = \left(\{ \bar{1}, \bar{2}, \bar{3}, \bar{4} \}, \cdot_5 \right) = \langle \bar{2} \rangle$

$$\mathbb{Z}_4 = \left(\{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \}, +_4 \right)$$

$$= \langle \bar{1} \rangle \quad \left[\begin{array}{l} \bar{1}^1 = \bar{1} \\ \bar{1}^2 = \bar{2} \\ \bar{1}^3 = \bar{3} \\ \bar{1}^4 = \bar{0} \end{array} \right]$$

$$\left[\begin{array}{l} \bar{2}^1 = 2 = \bar{2} \\ \bar{2}^2 = 4 = \bar{4} \\ \bar{2}^3 = 8 = \bar{3} \\ \bar{2}^4 = 16 = \bar{1} \end{array} \right]$$

So, U_5 and \mathbb{Z}_4 both are cyclic groups of order 4.

$\therefore \text{Aut}(\mathbb{Z}_5) \cong U_5 \cong \mathbb{Z}_4$ [\because Cyclic groups of same order are isomorphic]

$$\therefore \text{Aut}(\mathbb{Z}_5) \cong U_5 \cong \mathbb{Z}_4$$

$$\therefore \text{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4 \text{ (Proved)}$$

7) Show that,
 $\text{Aut}(\mathbb{Z}_8) \cong V$ [Klein's 4-group]

\Rightarrow We know, $\text{Aut}(\mathbb{Z}_n) \cong U_n \quad \forall n \in \mathbb{N}$

$$\therefore \text{Aut}(\mathbb{Z}_8) \cong U_8$$

Now, $U_8 = \left(\{ \bar{1}, \bar{3}, \bar{5}, \bar{7} \}, \cdot_8 \right)$

$$V = (\{e, a, b, c\}, \cdot)$$

U_8 and V are 2 non-cyclic groups of order 4. And for groups of order 4, there are only 2

types of groups upto isomorphism. One is the cyclic groups of order 4 which are isomorphic ^(type) to \mathbb{Z}_4 . And the other type is non-cyclic group of order 4 which is isomorphic to V (Klein's 4-group).

But Here, Both V and U_8 contains ~~1~~ One identity element whose order is 1 and ^{each of} the other 3 elements in each group is of order 2.

In U_8 ,	In V
$ \bar{1} = 1$	$ e = 1$
$ \bar{3} = 2$	$ a = 2$
$ \bar{5} = 2$	$ b = 2$
$ \bar{7} = 2$	$ e = 2$

$$\therefore U_8 \cong V$$

$$\Rightarrow \text{Aut}(\mathbb{Z}_8) \cong U_8 \cong V$$

$$\Rightarrow \text{Aut}(\mathbb{Z}_8) \cong V \text{ (Proved)}$$

8) Show that for any p being prime number,

$$|\text{Aut}(\mathbb{Z}_p)| = (p-1)$$

$$\Rightarrow \text{We know, } \text{Aut}(\mathbb{Z}_n) \cong U_n \quad \forall n \in \mathbb{N}$$

$$\therefore \text{For } p \text{ being a prime, } \text{Aut}(\mathbb{Z}_p) \cong U_p$$

Now, When two groups are isomorphic, then number of elements or, cardinality of those 2 groups become same.

$$\therefore |\text{Aut}(\mathbb{Z}_p)| = |U_p| = \phi(p) = (p-1)$$

~~$\phi(p)$~~ = number of elements prime

$\phi(p)$ = number of ~~real~~ natural numbers less than p and prime to p .

Q9) Prove that $\text{Inn}(S_3) \cong S_3 \cong \text{Aut}(S_3)$

\Rightarrow [The basic idea is to prove that $\text{Inn}(S_3) = \text{Aut}(S_3)$ and, $|\text{Inn}(S_3)| = |\text{Aut}(S_3)| = 6$ and $\text{Inn}(S_3)$ and $\text{Aut}(S_3)$ are both non-cyclic. Then the prove is complete.]

~~But~~ [Answer is still incomplete.]

\Rightarrow Let, $Z(S_3)$ be the Center of this group S_3 . Now, $Z(S_3)$ is the trivial subgroup of S_3 . $|Z(S_3)| = 1$.

Now, We know,

$$\therefore Z(S_3) = \{e\}$$

$$\frac{G}{Z(G)} \cong \text{Inn}(G)$$

$$\therefore \frac{S_3}{Z(S_3)} \cong \text{Inn}(S_3) \Rightarrow S_3 \cong \text{Inn}(S_3)$$

And $\text{Inn}(S_3) \cong \text{Aut}(S_3) \longrightarrow ??$ (How to prove this?)

Characteristic Subgroups

PAGE NO.

Prove that

10) Show that every characteristic subgroup of a group G is a normal subgroup of G .

\Rightarrow Let, H be a characteristic subgroup of G .

$$\therefore H < G \quad f(H) \subseteq H \quad \forall f \in \text{Aut}(G)$$

~~Let, $H < G$~~ . In particular, $\text{inn}(G) \in \text{Aut}(G)$

$$\therefore \text{inn}(H) \subseteq H$$

$$\Rightarrow I_g(H) = \{ghg^{-1} : g \in G\} \subseteq H$$

$$\therefore ghg^{-1} \in H \quad \forall g \in G \quad \therefore H \trianglelefteq G \quad (\text{Proved})$$

11) Prove that the center of a group (G) is also a characteristic subgroup. $(Z(G))$

$$\Rightarrow Z(G) = \{x \in G : xa = ax \quad \forall a \in G\}$$

$$\text{Let, } f \in \text{Aut}(G) \quad \text{Let, } x \in Z(G)$$

$$\therefore xa = ax \quad \forall a \in G$$

$$\Rightarrow f(xa) = f(ax)$$

$$\Rightarrow f(x)f(a) = f(a)f(x) \quad \forall a \in G$$

Let, $v \in G$ Since f is an automorphism on G so,
 \exists unique $u \in G$ s.t. $f(u) = v$

$$\begin{aligned} \therefore f(a)v &= f(a)f(u) = f(au) = f(ua) \\ &= f(u)f(a) \\ &= vf(a) \end{aligned} \quad \left[\begin{array}{l} \therefore a \in Z(G) \\ \therefore \forall x \in G \\ ax = xa \end{array} \right]$$

$$\therefore f(a) \in Z(G)$$

$$\therefore \cancel{a} \in Z(G) \Rightarrow f(a) \in Z(G)$$

$$\therefore f(Z(G)) \subseteq Z(G) \quad \forall f \in \text{Aut}(G)$$

$\therefore Z(G)$ is a characteristic subgroup of G .

Group Actions

5) Let, G be a group and $H < G$, let, $S = \{aH : a \in G\}$, Then \exists a homomorphism $\psi : G \rightarrow A(S)$ s.t. $\ker \psi \subseteq H$

→ This is also known as extended Cayley's theorem

⇒ Let, $g \in G$, we define, $\tau_g : S \rightarrow S$ s.t. $\tau_g(aH) = (ga)H$ $\forall aH \in S$

Let, $g_1, g_2 \in G$ and $aH \in S$,

$$\begin{aligned} \tau_{g_1 g_2}(aH) &= (g_1 g_2 a)H = g_1(g_2 aH) \\ &= g_1 \tau_{g_2}(aH) \\ &= \tau_{g_1} \circ \tau_{g_2}(aH) \end{aligned}$$

∴ $\forall g_1, g_2 \in G, \tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2}$

⑥

⑩ τ_g is well defined from $S \rightarrow S$,

~~if~~ for any two $a_1 H, a_2 H \in S$, if

$$\tau_g(a_1 H) = \tau_g(a_2 H)$$

$$\forall aH \in S \exists g^{-1}aH \in S$$

$$\Rightarrow (ga_1)H = (ga_2)H$$

$$\text{s.t. } \tau_g(g^{-1}aH) = (gg^{-1}a)H = aH$$

$$\Rightarrow a_1 H = a_2 H$$

$\therefore \tau_g$ is surjective

$\therefore \tau_g$ is injective.

$\therefore \tau_g$ is a bijection from S to S .

$\therefore \tau_g \in A(S)$ [Means τ_g is a permutation on S]

Let's define a mapping $\psi: G \rightarrow A(S)$ s.t. $\psi(g) = \tau_g$
s.t. $\psi(g) = \tau_g$.

$$\text{Then, for } g_1, g_2 \in G \quad \psi(g_1 g_2) = \tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2} \\ = \psi(g_1) \circ \psi(g_2)$$

$\therefore \psi$ is a homomorphism from $G \rightarrow A(S)$

$$\begin{aligned} \ker \psi &= \{ g \in G : \psi(g) = \text{id}_S \} \\ &= \{ g \in G : \psi(g) = \tau_g(aH) = aH, \forall aH \in S \} \\ &= \{ g \in G : (ga)H = aH \quad \forall aH \in S \} = \{ g \in G : gH = H \} \\ &\Rightarrow g \in H \quad \therefore \ker \psi \subseteq H \quad (\text{Proved}) \end{aligned}$$

[$A(S)$ = Set of all permutations on the set S .]

16) Let, G be a finite group and H be a proper subgroup of G of index n such that $|G|$ does not divide $n!$. Then G contains a non-trivial normal subgroup:

$$\Rightarrow \text{Given, } [G:H] = n = \frac{|G|}{|H|}$$

Let, $S = \{aH : a \in G\} \Rightarrow$ Set of all left cosets of H in G
 $\therefore |S| = n \Rightarrow |A(S)| = n!$

Now, By Cayley's extended theorem, $\exists \psi : G \rightarrow A(S)$ s.t.
 $\text{Ker } \psi \subseteq H$ $[\psi(g) = \tau_g \text{ where } g \in G, \text{ and } \tau_g : S \rightarrow S \text{ s.t.}$

By First isomorphism theorem,

$$\tau_g(aH) = (ga)H$$

$$\frac{G}{\text{Ker } \psi} \cong \text{A subgroup of } A(S)$$

$$\therefore \left| \frac{G}{\text{Ker } \psi} \right| \mid n!$$

The homomorphic image of order of the subgroup of $A(S)$ and the order of subgroup divides order of group.

$$\begin{aligned} \text{Now, } \left| \frac{G}{\text{Ker } \psi} \right| &= \frac{|G|}{|\text{Ker } \psi|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|\text{Ker } \psi|} \\ &= [G:H] \cdot [H:\text{Ker } \psi] \\ &= n \cdot [H:\text{Ker } \psi] \end{aligned}$$

[(unnecessary)]

Now, $|G| \neq n!$ so, $\frac{|G|}{|Ker \psi|} \nmid n!$

PAGE NO.

$$\Rightarrow |Ker \psi| > 1$$

$\therefore Ker \psi$ is not the trivial subgroup of G .
So, $Ker \psi$ is a proper subgroup of G and $Ker \psi$ is always a normal subgroup of G .

\therefore We have found a non-trivial normal subgroup of G . (Proved)

17) Let, S be a finite G -set, where G is a group of order p^n . such that $p \nmid |S|$.
show that $\exists a \in S$ s.t. a is fixed.

\Rightarrow We know that,

$$|S| = \sum_{a \in A} |[a]|$$

$$= \sum_{a \in A} [G : G_a]$$

$$= |S_0| + \sum_{a \in A - S_0} [G : G_a]$$

$$= |S_0| + \sum_{a \in A - S_0} \frac{|G|}{|G_a|}$$

(P.T.O)

$A =$ A subset of S containing only one element from each orbit

$[a] \rightarrow$ orbit of G on S containing a .

$[a \in S]$

$\because |[a]| = [G : G_a]$
where $G_a =$ stabilizer of a
for a fixed $a \in S$, $[a \in S]$
 $G_a = \{g \in G : ga = a\}$

$S_0 = \{a \in S : ga = a \forall g \in G\}$

Now, G_a is a subgroup of G for all $a \in S$.

$$|G| = p^n \therefore |G_a| \mid |G|$$

We can clearly see that,
 $[G : G_a] = p^k, k \geq 0$

$$\therefore |S| = |S_0| + pM \left[\because p \mid \sum_{a \in A-S_0} [G_a; G_a] \right]$$

$$\Rightarrow p \mid (|S| - |S_0|)$$

$$\text{Now, } p \nmid |S| \Rightarrow p \nmid |S_0|$$

You can check it yourself
if you have any doubt.

$$\therefore |S_0| \geq 1 \text{ means } |S_0| \neq 0$$

We saw that,

$$[G_a; G_a] = \frac{|G_a|}{|G_a|} = p^k$$

for some $k \geq 2$

[Forever at S]
or, to be precise,
 $\forall a \in A-S_0$

$$\therefore \sum_{a \in A-S_0} [G_a; G_a] = pM$$

M being some
natural number

Because $p > 1$, $p \nmid 0$
 $\forall p$ being prime
So, eventually $p \nmid |S_0|$
implies that $|S_0| \geq 1$
or, $|S_0| \neq 0$

Again, for $a \in S_0$ we
will see that,
 $[a] = [G_a; G_a] = 1 \quad \forall a \in S_0$
 $\therefore \sum_{a \in S_0} [G_a; G_a] = |S_0|$
(by common sense)

$\therefore |S_0| \geq 1$ means that ~~So~~ there exists
at least one element in S such that a is fixed
by G_a .
(a)

18) Let, G be a ~~prime~~ finite group, Let, $H < G$, $[G:H] = p$ where p is the smallest prime dividing $|G|$. Show that $H \trianglelefteq G$

(Very Hard)

\Rightarrow Just same as problem number 16. We will get, By Cayley's extended theorem, $\exists \psi: G \rightarrow A(S)$ s.t. $\ker \psi \leq H$ $[\psi(g) = \gamma_g \text{ where } g \in G \text{ and } \gamma_g(aH) = (ga)H \forall aH \in S]$

By given problem,

$$|S| = p$$

$$\therefore |A(S)| = p!$$

$S = \{aH : a \in G\}$
 $A(S) = \text{Set of permutation on the set } S.$

$$\therefore \left| \frac{G}{\ker \psi} \right| \mid p!$$

Let, $\left| \frac{G}{\ker \psi} \right| = \cancel{p!} \cdot n$ for some $n \in \mathbb{N}$

$$\begin{aligned} \left| \frac{G}{\ker \psi} \right| &= \frac{|G|}{|\ker \psi|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|\ker \psi|} \\ &= [G:H] \cdot [H:\ker \psi] \\ &= p \cdot [H:\ker \psi] \end{aligned}$$

$\Rightarrow \frac{p!}{p} = p$

$\Rightarrow \left| \frac{G}{\ker \psi} \right| \geq n \Rightarrow [G:H] \cdot [H:\ker \psi] = n \geq p$

Now, let, $n = p_1 p_2 \dots p_k$ $[p_i \text{ is a prime for all } i \in \{1, 2, \dots, k\}]$

Now, p is the smallest prime dividing $|G|$.

So, By observation we can conclude that $p \leq p_i \forall i \in \{1, 2, \dots, k\}$

and hence, $n \mid p!$ ~~for $p \leq n$~~

$$\Rightarrow \phi = p_1 \Rightarrow p_1 p_2 \dots p_k \mid p!$$

So, We observe that, $p = p_1$ [$p_1 \rightarrow$ The smallest prime ~~is~~ out of all p_i 's.]

$$\therefore n = p$$

$$\therefore \left| \frac{G}{\text{Ker } \psi} \right| = n = p$$

$$\Rightarrow [G : H] \cdot [H : \text{Ker } \psi] = p \Rightarrow p \cdot [H : \text{Ker } \psi] = p \Rightarrow [H : \text{Ker } \psi] = 1 \Rightarrow H = \text{Ker } \psi$$

$$\Rightarrow H = \text{Ker } \psi \text{ and } \text{Ker } \psi \trianglelefteq G \therefore H \trianglelefteq G \text{ (Proved)}$$

19) Let, G be a group of order pn , p is a prime and $p > n$. If H is a subgroup of G , $|H| = p$. Prove that $H \trianglelefteq G$.

$$\Rightarrow \text{Again, Let, } S = \{aH : a \in G\} \quad |S| = [G : H] = \frac{|G|}{|H|} = \frac{pn}{p} = n$$

$$\therefore |A(S)| = n!$$

By extended Cayley's theorem, $\exists \psi : G \rightarrow A(S)$ s.t.

$$\text{Ker } \psi \leq H, \quad \left[\psi(g) = \tau_g \text{ where } g \in G \quad \text{For any } g \in G, \right.$$

$$\left. \tau_g(aH) = (ga)H \quad \forall aH \in S \right]$$

$$\text{Now, } \text{Ker } \psi \leq H \quad |H| = p$$

$$\therefore |\text{Ker } \psi| = \{1, p\}$$

If $|\text{Ker } \psi| = 1$ means if $\text{Ker } \psi = \{e\}$ then,

By first isomorphism theorem,

$$\frac{G}{\text{Ker } \psi} \cong \text{A Sub group of } A(S)$$

$$\Rightarrow \left| \frac{G}{\text{Ker } \psi} \right| \mid n! \Rightarrow \frac{|G|}{|\text{Ker } \psi|} \mid n! \Rightarrow |G| \mid n!$$

[\therefore We assumed $|\text{Ker } \psi| = 1$]

$$\therefore pn | n!$$

$$\Rightarrow p | (n-1)! \quad \text{Now, } p \text{ is a prime and } p > n$$

$$\text{So, } p \nmid (n-1)!$$

This creates contradiction.

\therefore Our assumption was wrong. So, $|\ker \psi| \neq 1$ and $|\ker \psi| = p$

$$\therefore H = \ker \psi$$

$$= |H|$$

$$\text{Now, } \ker \psi \trianglelefteq G \Rightarrow H \trianglelefteq G \text{ (Proved)}$$

20) State and prove Cayley's theorem.

\Rightarrow Cayley's theorem: For any group (G, \cdot) , there exists an isomorphism from G to $F(G)$, where $F(G)$ is a group subgroup of $A(G)$ [we have to prove this too].
[$A(G) \rightarrow$ The set of all permutations on G]

Proof: $F(G) = \{f_a : a \in G\}$

Let, $a \in G$,

$$\text{For any } g \in G, f_a(g) = ag$$

$$\text{Let, for } b, c \in G, f_b, f_c \in F(G)$$

Then, for any $g \in G$,

$$f_b \circ f_c^{-1}(g) = f_b \circ f_{c^{-1}}(g) = f_b[c^{-1}g] = bc^{-1}g = f_{bc^{-1}}(g)$$

$$\therefore f_b, f_c \in F(G) \Rightarrow f_b \circ f_c^{-1} \in F(G)$$

$$\therefore (F(G), \circ) \text{ is a subgroup of } (A(G), \circ)$$

Let, $\tau_g: G \rightarrow G$ s.t. $\tau_g(a) = ga \quad \forall a \in G$ for any $g \in G$

We observe that, $\tau_{g_1 g_2}(a) = g_1 g_2(a) = g_1 \tau_{g_2}(a)$
 $[\text{for any } g_1, g_2 \in G] \quad = \tau_{g_1} \circ \tau_{g_2}(a)$

$\therefore \tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2} \quad [\tau_g \text{ is a permutation on } G] \quad \forall a \in G$
 $[\tau_g \in A(G)]$

Now, let, $\psi: G \rightarrow F(G)$ s.t. $\psi(g) = \tau_g \quad \forall g \in G$

Then, we see,

$$\psi(g_1 g_2) = \tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2} = \psi(g_1) \psi(g_2)$$

$\therefore \psi$ is a homomorphism from G to $F(G)$

$$\text{Let, } \psi(g_1) = \psi(g_2)$$

$$\Rightarrow \tau_{g_1}(a) = \tau_{g_2}(a) \quad \forall a \in G$$

$$\Rightarrow g_1 a = g_2 a \quad \forall a \in G$$

$$\Rightarrow g_1 = g_2 \quad [\text{By left cancellation property of group}]$$

$\therefore \psi$ is monomorphism.

Again, for any $\tau_{g_n} \in F(G) \exists g_n \in G$ s.t.

$$\psi(g_n) = \tau_{g_n}$$

$\therefore \psi$ is an epimorphism too.

$\therefore \psi$ is an isomorphism from G to $F(G)$.

(Proved)

21) Let, G be a group of order $2m$, where m is an odd integer.
Show that G has normal subgroup of order m .

\Rightarrow By ~~extended~~ Cayley's theorem, $\exists \psi$, a homomorphism from $G \rightarrow A(G)$ or, an epimorphism (ψ) from G to a subset of $A(G)$. s.t. $\psi(g) = \tau_g \quad \forall g \in G$
(H)

for any $g \in G$, $\tau_g(a) = ga \quad \forall a \in G$

Now, $|G| = 2m$, ~~so~~ and m is an odd integer.

$\therefore \exists g \in G$ s.t. $|g| = 2 \quad \therefore g^2 = e$

$\therefore \tau_g(a) = g(a) \quad \forall a \in G$

$\Rightarrow \tau_g \circ \tau_g(a) = g(ga) = g^2 a = a = \tau_G(a)$
the product of transpositions

$\therefore \tau_g$ is of the form of (ga) . ~~so the~~

Since, $|G| = 2m$. The number of transpositions appearing in the factorization is m . Thus, τ_g is an odd permutation.

Now, define, $H = \{1, -1\}$

H is a group under multiplication.

$\psi: G \rightarrow H$ s.t. $\begin{cases} \psi(\sigma) = 1 & \text{for } \sigma \text{ being even permutation on } G \\ \psi(\sigma) = -1 & \text{, } \sigma \text{, odd permutation} \end{cases}$

$$\therefore \frac{G_2}{\ker \psi} \cong H \quad [\text{By first isomorphism theorem}]$$

PAGE NO.

$$\Rightarrow \left| \frac{G_2}{\ker \psi} \right| = |H| = 2$$

$$\Rightarrow \frac{|G_2|}{|\ker \psi|} = 2 \Rightarrow \frac{2m}{|\ker \psi|} = 2 \Rightarrow |\ker \psi| = m$$

Now, $\ker \psi \trianglelefteq G_2$

\therefore We have found the normal subgroup of order m .

22) Let, G be a group of order 70 such that G has a subgroup of order 14. Show that G has non trivial normal subgroup.

\Rightarrow By previous problem, we see if $|G| = 2m$ where m is an odd integer, then, there exists a normal subgroup of order m .

Now, $|G| = 70 = 2 \times 35$, 35 is an odd integer.

$\therefore G$ has a normal subgroup of order 35.

$\therefore G$ has a non-trivial subgroup. (Proved).

Commutator group

Let, C be the commutator subgroup of a group G . Then,

i) $C \trianglelefteq G$

ii) ~~G is abelian~~ $\frac{G}{C}$ is abelian.

iii) let, $N \trianglelefteq G$, $\frac{G}{N}$ is abelian iff $C \subseteq N$.

\Rightarrow i) For any $a, b \in G$, $aba^{-1}b^{-1} \in C$

let, $x \in G$

$$\begin{aligned} \therefore xaba^{-1}b^{-1}x^{-1} &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})(xb^{-1}x^{-1}) \\ &= (xax^{-1})(xbx^{-1})(xa^{-1}x^{-1})^{-1}(xb^{-1}x^{-1})^{-1} \\ &\in C \end{aligned}$$

\therefore for any $x \in G$

$$xCx^{-1} \subseteq C \quad \therefore C \trianglelefteq G \text{ (Proved)}$$

ii) For any $a, b \in G$, $aba^{-1}b^{-1} \in C$

$$\Rightarrow ab(ba)^{-1} \in C$$

$$\Rightarrow Cab = Cba \quad [\because C \trianglelefteq G]$$

$$\Rightarrow Ca * Cb = Cb * Ca \quad \left[\begin{array}{l} \because ab^{-1} \in C \\ \Rightarrow Ca = Cb \end{array} \right]$$

$$[\because C \trianglelefteq G \therefore \frac{G}{C} \text{ exists and in } \frac{G}{C}, Cab = Ca * Cb]$$

i. $\frac{G}{e}$ is abelian. (Proved)

iii) $N \trianglelefteq G$, let, $\frac{G}{N}$ is abelian.

$$\therefore aN * bN = bN * aN \quad \forall a, b \in G$$

$$\Rightarrow abN = baN \quad \forall a, b \in G$$

$$\Rightarrow ab(ba)^{-1} \in N \quad \forall a, b \in G$$

$$\Rightarrow aba^{-1}b^{-1} \in N \quad \forall a, b \in G$$

$$\Rightarrow e \in N$$

Conversely, If, $e \subseteq N$ then, for any $a, b \in G$

$$aba^{-1}b^{-1} \in N \Rightarrow ab(ba)^{-1} \in N$$

~~$$abN = baN$$~~

$$\Rightarrow abN = baN$$

$$\Rightarrow aN * bN = bN * aN$$

$\therefore \frac{G}{N}$ is abelian. (Proved)

⑩

2) The Commutator Subgroup e of G is a characteristic subgroup of G .

\Rightarrow Let, $a, b \in G$, $f \in \text{Aut}(G)$

$$\therefore aba^{-1}b^{-1} \in e$$

$$\begin{aligned} \therefore f(aba^{-1}b^{-1}) &= f(a)f(b)f(a^{-1})f(b^{-1}) \\ &= f(a)f(b)[f(a)]^{-1}[f(b)]^{-1} \end{aligned}$$

Now, for any $a, b \in G$ and $f \in \text{Aut}(G)$

$$f(a), f(b), [f(a)]^{-1}, [f(b)]^{-1} \in G$$

PAGE NO.

$$\therefore f(a) f(b) [f(a)]^{-1} [f(b)]^{-1} \in C \quad \forall a, b \in G \text{ and } \forall f \in \text{Aut}(G)$$

$$\therefore f(ab a^{-1} b^{-1}) \in C \quad \forall a, b \in G \text{ and } \forall f \in \text{Aut}(G)$$

$$\therefore f(C) \subseteq C \quad \forall f \in \text{Aut}(G)$$

$\therefore C$ is a characteristic subgroup. (Proved)